ShoreTel® 8.1

Maintenance Guide

ShoreTel®

Document and Software Copyrights

Copyright © 1998–2008 by ShoreTel, Inc., Sunnyvale, California, U.S.A. All rights reserved. Printed in the United States of America. Contents of this publication may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior written authorization of ShoreTel, Inc.

ShoreTel, Inc. reserves the right to make changes without notice to the specifications and materials contained herein and shall not be responsible for any damage (including consequential) caused by reliance on the materials presented, including, but not limited to, typographical, arithmetic, or listing errors.

Trademarks

ShoreTel®, ShoreCare®, ShoreWare®, ShoreGear® and ControlPoint® are registered trademarks of ShoreTel, Inc. in the United States and/or other countries. ShorePhone™ is a trademarks of ShoreTel, Inc. in the United States and/or other countries. All other copyrights and trademarks herein are the property of their respective owners.

Patents

This product is covered by one or more of the following patents: United States patent 6,996,059, United States patent 7,003,091, United States patent 7,167,486, United States patent 7,379,540, and United States patent 7,386,114. ShoreTel, Inc. All rights reserved.

Version Information

ShoreTel Maintenance Guide
Revision 2
Part Number: 800-1229-01
Date: September 25, 2008

Company Information

ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, California 94085

(408) 331-3300
(408) 331-3333 fax

www.shoretel.com

Table of Contents

TABLE OF CONTENTS i

CHAPTER 1: INTRODUCTION 1

1.1 Conventions . . . 1
1.1.1 Syntax . . . 1
1.2 For More Information . . . 1

CHAPTER 2: SHORETEL ARCHITECTURE 3

2.1 Overview . . . 3
2.1.1 ShoreWare Servers . . . 3
2.1.2 ShoreGear Voice Switches . . . 3
2.1.3 IP Endpoints . . . 3
2.1.4 ShoreWare Client Applications . . . 4
2.2 ShoreTel Distributed IP Voice Architecture . . . 4
2.2.1 Distributed Applications Platform . . . 5
2.2.2 Distributed Call Control . . . 5
2.2.3 Single System Management . . . 6
2.3 ShoreTel System Communications . . . 7
2.3.1 Call Control . . . 7
2.3.2 Configuration . . . 10
2.3.3 TAPI . . . 11
2.3.4 Media . . . 12
2.4 System Reliability . . . 13
2.4.1 Distributed Switch Control . . . 13
2.4.2 Embedded IP Phone Display Driver . . . 14
2.4.3 Public Switched Telephone Network (PSTN) Failover . . . 15
2.4.4 Distributed CDR . . . 15
2.4.5 For More Information . . . 15
2.5 Call Scenarios . . . 15
2.5.1 On-hook Call from Personal Call Manager . . . 16
2.5.2 Quick Dial Call from Personal Call Manager . . . 17
2.5.3 Inbound Call from a Trunk . . . 18
2.6 Reference . . . 18
2.6.1 TCP/IP Ports Used by the ShoreTel System . . . 18

CHAPTER 3: SHOREWARE SERVERS 23

3.1 Overview . . . 23
3.1.1 Headquarters Server . . . 23
3.1.2 Remote Servers . . . 23
3.1.3 Configuration Communications . . . 24
3.1.4 Call Control Communications . . . 26
3.1.5 Media Communications . . . 27
3.1.6 Integrated Server Applications . . . 28
3.2 Maintenance . . . 30

3.2.1 Server Software Upgrades . . . 30
3.2.2 Recommended Files to Backup . . . 30
3.3 Diagnostic and Troubleshooting Information . . . 31
3.3.1 Installer Logging . . . 31
3.3.2 Using Quick Look . . . 32
3.3.3 Using the Event Log . . . 32
3.3.4 Using the System Logs . . . 32
3.3.5 Using the Trunk Test Tool . . . 38
3.3.6 Using TapiTest . . . 39
3.3.7 Using the cfg Utility . . . 39
3.3.8 Using Dr. Watson . . . 41
3.4 Reference . . . 43
3.4.1 Services (Processes) . . . 43
3.4.2 ShoreWare Server File System . . . 43
3.4.3 Registry . . . 47
3.4.4 ShoreTel Release Numbering Scheme . . . 47

CHAPTER 4: SHOREGEAR SWITCHES 49

4.1 Overview . . . 49
4.2 Maintenance . . . 50
4.2.1 ShoreGear Firmware Upgrades . . . 50
4.2.2 ShoreGear Switch Boot Options . . . 51
4.2.3 ShoreGear Switch Configuration Reset . . . 56
4.2.4 ShoreGear Switch Utilities . . . 57
4.3 Diagnostics . . . 58
4.3.1 Using the Switch Trunk Debugging Tools . . . 58
4.3.2 Using VxWorks Command Line Interface . . . 59
4.3.3 Connecting to a ShoreGear Voice Switch . . . 67
4.3.4 Power over Ethernet Switches . . . 67

CHAPTER 5: VOICEMAIL MODEL SWITCHES 69

5.1 Introduction . . . 69
5.2 Utilities . . . 69
5.2.1 Accessing Voicemail Model Switch Utilities . . . 69
5.2.2 Switch Utilities . . . 72
5.2.3 Server Utilities . . . 74
5.3 Booting and Restarting . . . 75
5.3.1 Description . . . 75
5.3.2 Specifying a Static IP Address . . . 75
5.3.3 Reboot Methods . . . 76
5.4 Diagnostics and Repair . . . 77
5.4.1 Using Switch Trunk Debug Tools . . . 77
5.4.2 Creating an Ethernet Trace File . . . 77
5.4.3 Recording Audio from a Switch Port . . . 78
5.4.4 Using Traceroute . . . 78
5.4.5 Reformatting the Compact Flash . . . 79
5.5 Reference . . . 80
5.5.1 STCLI Command Descriptions . . . 80
5.5.2 SVCCLI Command Descriptions . . . 82
5.5.3 CLI . . . 87
5.5.4 Cfg Utility . . . 91
5.5.5 UBOOT . . . 92

5.5.6 Burnflash . . . 93
5.5.7 ipbxctl . . . 93
5.5.8 regedit . . . 94
5.5.9 ShoreWare File System . . . 96

CHAPTER 6: IP ENDPOINTS 97

6.1 Overview . . . 97
6.1.1 IP Phones . . . 97
6.1.2 Boot Process . . . 100
6.2 Maintenance . . . 100
6.2.1 IP Phone Firmware Upgrades . . . 100
6.3 Diagnostics . . . 100
6.3.1 Viewing System IP Phones . . . 100
6.3.2 Onscreen Error Messages . . . 101
6.3.3 Diagnostic and Failure Messages . . . 101
6.3.4 IP100 Phone Troubleshooting . . . 102
6.3.5 Troubleshooting the IP Phone Display . . . 103
6.3.6 Manually Configuring the Phones . . . 105
6.3.7 Displaying IP110/115/212k/230/530/560/560g Settings . . . 106
6.3.8 Resetting the IP110/115/212k/230/530/560/560g . . . 107
6.4 Diagnostics & Config for IP110/115/212k/230/530/560/560g . . . 107
6.4.1 Boot Configuration Operation . . . 107
6.4.2 IP Phone Configuration Files . . . 107
6.4.3 Other Customizable Parameters . . . 110
6.4.4 DHCP Site Specific Options . . . 117
6.4.5 PhoneCTL Command Line Tool . . . 119
6.5 ShoreTel Conference Bridges . . . 123
6.5.1 SoftPhone . . . 123
6.6 Reference . . . 124
6.6.1 Dial Tone Behavior . . . 124
6.6.2 Manually Configuring the ShorePhone-IP100 . . . 125
6.6.3 Setting IP100 Phone Configuration from the Phone Interface . . . 125

CHAPTER 7: SHORETEL CLIENT APPLICATIONS 131

7.1 Overview . . . 131
7.1.1 Call Manager Application Suite . . . 131
7.1.2 Theory of Operations . . . 131
7.2 Diagnostics . . . 132
7.2.1 Troubleshooting Login or Startup Problems . . . 132
7.2.2 Troubleshooting Telephony Problems . . . 135
7.2.3 Confirming TAPI Operations . . . 135
7.2.4 Troubleshooting Caller ID Problems . . . 136
7.2.5 Troubleshooting Configuration Problems . . . 137
7.2.6 Troubleshooting MAPI Contact Import Problems Using *SHAdrTst.exe* . . . *137*
7.2.7 Using the History File . . . 138
7.2.8 Using Log Files . . . 138
7.3 Reference . . . 139
7.3.1 Call Activity Log File . . . 139
7.3.2 Customizing StartCli . . . 139
7.3.3 The Setup Wizard . . . 140

APPENDIX A: EVENT CODES 143

A.1 Event Types . . . 143
A.2 Using the Event Code Tables . . . 143
A.2.1 Reading the Event Tables . . . 143
A.2.2 About Severity Levels . . . 144
A.3 Switches . . . 145
A.4 TMS . . . 155
A.5 Voice Mail . . . 162
A.6 TDI Media . . . 167
A.7 Event Watch . . . 169
A.8 Configuration Administration . . . 170
A.9 Port Mapper . . . 171
A.10 Trigger Server . . . 172
A.11 Distributed Routing Service (DRS) . . . 173
A.12 Kadota Utility . . . 174
A.13 Call Accounting . . . 175
A.14 Workgroup Server . . . 176
A.15 CSIS . . . 177
A.16 IP Phone Console Server (IPCS) . . . 178
A.17 IP Phone Display Server (IPDS) . . . 179

APPENDIX B: DCOM PERMISSIONS 183

B.1 Introduction . . . 183
B.2 Editing DCOM Permissions . . . 183
B.2.1 My Computer Properties . . . 184
B.2.2 TriggerServer Properties . . . 185
B.2.3 Kadota Utilities Properties . . . 187
B.2.4 TMSManager2 Properties . . . 189
B.2.5 ZinManager Properties . . . 191

CHAPTER C: SHOREGEAR SWITCHES 195

C.1 Switch Models . . . 195
C.1.1 ShoreGear 1-U Half Width Voice Switches . . . 195
C.1.2 ShoreGear Voicemail Model Voice Switches . . . 196
C.1.3 ShoreGear 1-U Full Width Voice Switches . . . 197
C.1.4 ShoreGear IPBX Voice Switches . . . 197
C.2 Specifications – SG 1-U Half-Width Switches . . . 199
C.2.1 ShoreGear 90 Voice Switch . . . 199
C.2.2 ShoreGear 90BRI Voice Switch . . . 202
C.2.3 ShoreGear 50 Voice Switch . . . 205
C.2.4 ShoreGear 30 Voice Switch . . . 208
C.2.5 ShoreGear 30BRI Voice Switch . . . 212
C.2.6 ShoreGear 220T1 Voice Switch . . . 215
C.2.7 ShoreGear 220T1A Voice Switch . . . 218
C.2.8 ShoreGear-220E1 Voice Switch . . . 221
C.2.9 ShoreGear T1k Voice Switch . . . 224
C.2.10 ShoreGear E1k Voice Switch . . . 227
C.3 Specifications – SG Voice Model Switches . . . 231
C.3.1 ShoreGear 90V Voice Switch . . . 231

C.3.2 ShoreGear 90BRIV Voice Switch 234
C.3.3 ShoreGear 50V Voice Switch 237
C.4 Specification – SG 1U Full Width Switches 241
C.4.1 ShoreGear 120 Voice Switch 241
C.4.2 ShoreGear 24A Voice Switch 244
C.4.3 ShoreGear 60 Voice Switch 247
C.4.4 ShoreGear-T1 and ShoreGear E1 Voice Switches 254
C.5 Specification – IPBX Switches 257
C.5.1 IPBX-24 Voice Switch 257
C.5.2 IPBX-T1 and IPBX-E1 Voice Switch 260

CHAPTER 1

Introduction

The ***ShoreTel 8 Maintenance Guide*** provides a valuable resource for troubleshooting and solving problems that can arise in a highly complex system such as ShoreTel 7.

1.1 Conventions

The guide uses the following text elements to identify special information.

- `Courier –` Code examples and information that you type appears in this font.
- **UPPERCASE –** Words that appear in uppercase identify keywords related to the ShoreTel 8 system.

WARNING This cautionary note alerts you to situations where you can lose data or damage equipment by failing to follow instructions.

1.1.1 Syntax

The guide uses these typographic conventions to clarify syntax:

- *Italic* – Indicates parameters that are variable and can change depending on usage. Also used to identify documents and path names.
- < > – Brackets surround items that are supplied by a user, or are variables that appear in event codes.

1.2 For More Information

In addition to the ***ShoreTel 8 Maintenance Guide***, ShoreTel publishes other documents that can help you solve problems and maintain high system availability, including:

- ***ShoreTel 8 Planning and Installation Guide*** a comprehensive guide to planning and implementing a full-featured, enterprise-class VoIP system.
- ***ShoreTel 8 Administration Guide*** a detailed reference guide to administering a ShoreTel system.\

CHAPTER 2

ShoreTel Architecture

2.1 Overview

The ShoreTel system is a highly distributed, highly reliable voice communication system. A complete ShoreTel system is composed of four fundamental components:

- ShoreWare servers
- ShoreGear voice switches
- IP endpoints such as IP phones
- Client applications

The system may also include:

- ShoreTel Converged Conference Solution
- ShoreTel Contact Center Solution

The ShoreTel system's components interact with each other in a distributed environment. The heart of the architecture is the Telephony Management Service (TMS), which provides overall control for the entire ShoreTel system.

The administrative client, ShoreWare Director, is used to configure and manage the whole system.

Figure 2-1 shows the various components of a ShoreTel system and how they interact with the public switched telephone network (PSTN) and IP-based networks.

2.1.1 ShoreWare Servers

Each ShoreTel system has a main server called the Headquarters (HQ) server. Systems may optionally include distributed servers.Each server provides a local instance of TMS that supports applications such as voice mail and Personal Call Manager. Each instance of TMS manages its local SoftSwitch and can be configured to manage ShoreGear voice switches as well. The distributed servers continue to rely on the HQ server for configuration changes, but otherwise can operate independently of the HQ server.

2.1.2 ShoreGear Voice Switches

ShoreTel ShoreGear voice switches provide physical connectivity for the PSTN and analog phones, and logical connectivity for IP endpoints on a reliable, highly scalable platform for the ShoreTel call control software. The ShoreGear voice switches receive their configuration information via TMS.

2.1.3 IP Endpoints

The ShoreTel system manages calls and applications for three types of IP endpoints: IP phones, SoftPhones, and ShoreTel converged conference bridges. IP endpoints are identified by IP address and can exist anywhere on the network.

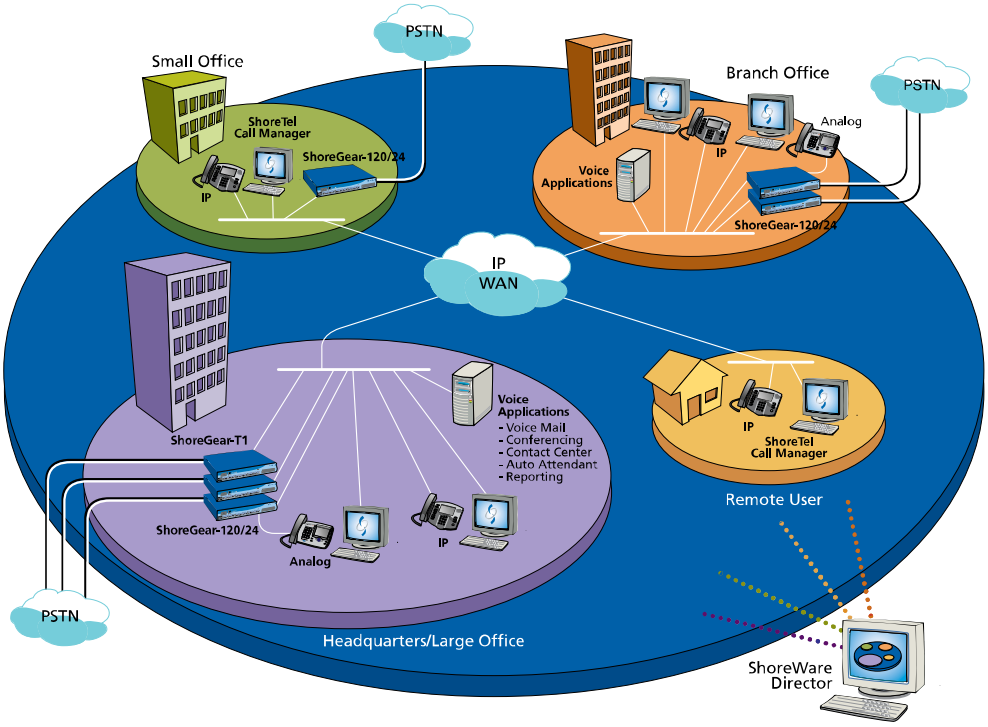

Figure 2-1 ShoreTel System

2.1.4 ShoreWare Client Applications

The client applications, including Personal Call Manager, Voice Mail Viewer, and Operator client, interact with the TMS using the Telephony Application Programming Interface (TAPI) for call handling and the Client-Server Internet Service (CSIS) interface for data handling. Client applications use CSIS to retrieve and update data through the ZIN Manager (DCOM) interface.

2.1.4.1 Personal Call Manager

The Personal Call Manager (PCM) provides desktop call control as well as voice mail, directory, and call logging features. Microsoft Outlook users can integrate their voicemail, contacts, and calendar with the ShoreTel 7 system.

2.2 ShoreTel Distributed IP Voice Architecture

The ***ShoreTel 8*** system is a completely distributed voice communication solution with no single point of failure, which is layered on top of your IP network. Central to the system is the standards-based Distributed IP Voice Architecture (Figure 2-2), which uniquely distributes call control intelligence to voice switches connected anywhere on the IP network. In addition, the Distributed IP Voice Architecture distributes voice applications, including voice mail systems and automated attendants, to servers across locations, rather than centralizing applications at the network core.

The resulting solution provides a single image system for all locations and voice applications.

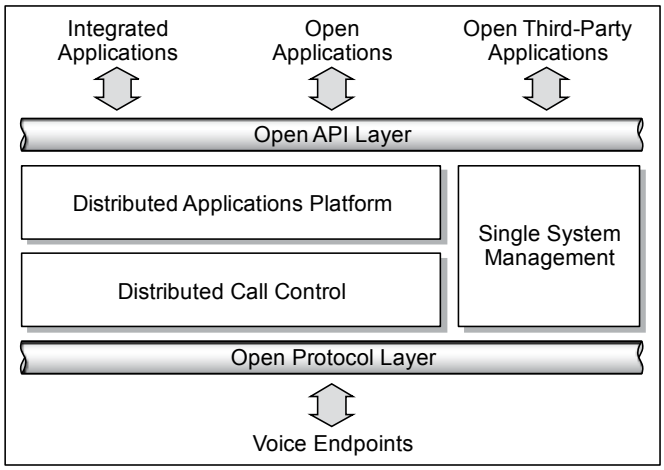

Figure 2-2 The Distributed IP Voice Architecture of the *ShoreTel 8* System

2.2.1 Distributed Applications Platform

The ShoreTel system's ability to support applications on distributed servers across the enterprise while maintaining a single, cohesive system depends on the ShoreWare Telephony Management Service (TMS) and the ShoreWare Distributed Telephony Application Service (DTAS).

TMS runs on each ShoreWare server and observes all call activity for the SoftSwitch and ShoreGear voice switches it manages. DTAS also runs on each ShoreWare server and directs requests to the appropriate TMS. By putting a server at the same site as the users, applications such as voice mail and the Personal Call Manager can run regardless of the network availability to the Headquarters server. In addition, by hosting applications, services, and APIs on multiple ShoreWare servers, the system can scale as necessary by adding ShoreWare servers.

The ShoreWare TMS/DTAS software exposes a Telephony Application Programming Interface (TAPI) for call control, and a TAPI WAV interface for media playing and recording. These open APIs allow value-added applications to be added to the ShoreTel system to provide voice services.

Even when there are multiple application servers, the ShoreTel system is still managed and behaves as a single image system with complete feature transparency between sites.

2.2.2 Distributed Call Control

Distributed call control is a key concept of the ShoreTel system. Based on the industry-standard SIP protocol, ShoreTel's distributed call control software runs on every ShoreGear voice switch in the ShoreTel system. Each switch call control element manages the call setup and teardown, including features such as transferring, conferencing, and forwarding calls, using call permissions, and call routing for the endpoints that it supports (both analog and IP).

The voice switches communicate on a peer-to-peer basis, eliminating any single point of failure. For instance, if one ShoreGear voice switch goes offline, all other ShoreGear voice switches continue operating. When the voice switch comes back online, it rejoins the voice network with no impact on system operation. There is no server involved with the basic telephony, so the system delivers levels of availability unmatched by even legacy vendors.

ShoreGear switches build an internal routing database from the peer-to-peer communication with other switches. Each ShoreGear switch contains routing information for all endpoints in the system, including information regarding trunk selection for outbound calls (unless Distributed Routing Service has been enabled. See Section 2.2.2.1 on page 6.) When a user places a call from any extension, each switch can route the call to the correct ShoreGear switch based on its internal routing database. Sites can typically support up to 60 ShoreGear voices switches depending on the system configuration.

The heart of the ShoreTel 7 system is the distributed call control software, which runs on the ShoreGear voice switches on top of VxWorks™ a real-time operating system. Each call control element manages the call setup and call teardown, including features such as transfer, conference, forward, call permissions, and call routing. The voice switches communicate on a peer-to-peer basis, eliminating any single point of failure. For instance, if one ShoreGear voice switch goes offline, all other ShoreGear voice switches continue operating. When the voice switch comes back online, it rejoins the voice network with no impact on system operation. There is no server involved with the basic telephony, so the system delivers levels of availability unmatched by even legacy vendors.

2.2.2.1 Distributed Routing Service

Distributed Routing Service (DRS) allows larger systems to scale beyond 60 switches up to a total of 500 switches (including SoftSwitches). The Distributed Routing Service is optional on systems up to 60 switches, but must be enabled on systems with 60 or more switches.

When Distributed Routing Service is enabled, ShoreGear switches only exchange routing information with other switches configured in the same site, rather than exchanging information with every switch in the system. Although each ShoreGear switch only maintains routing information within its site, each ShoreWare server also includes an instance of the Distributed Routing Service, which maintains system-wide routing information. When site-to-site calls are initiated, ShoreGear switches contact the Distributed Routing Service in order to find the ShoreGear switch or switches necessary to complete the call.

In a system with more than one ShoreWare server, the ShoreGear switches may contact an alternate instance of the routing service if the primary instance is unreachable. ShoreWare servers have a hierarchical relationship, with the Headquarters server at the top of the hierarchy. As you add servers to the system using ShoreWare Director, you define the order of the servers in relation to the Headquarters server and the various sites in your system. Initially, the switches try to contact the nearest instance of the Distributed Routing Service in the hierarchy. If that instance of DRS is unreachable, the switch contacts the instance of DRS at the parent server in the hierarchy as a fallback. If both instances of DRS are unreachable, the switch makes a best effort to route the call based on its internal routing tables built from communicating with peer ShoreGear switches at the same site.

If the call is an external call, the call may be routed out a local trunk even though it may not be the lowest cost. If the call is an internal call, the call will be redirected to the Backup Auto-Attendant.

2.2.3 Single System Management

The ***ShoreTel 8*** system provides a browser-based network management tool called ShoreWare Director that provides a single management interface for all voice services and applications across all locations. Although there are multiple servers and switches to support the services and applications, the ***ShoreTel 8*** system provides a single image system across your entire network.

Integrated management enables a change to propagate dynamically across the system each time a modification is made on the ***ShoreTel 8*** system. When you add a new user to the system, that user automatically receives a dialing plan, voice mail, an extension, a mailbox, an Auto-Attendant profile, and an email reminder to download the desktop software. In addition, the user can be added to a Workgroup, if needed. You add new users and place them in Workgroups from a single management screen.

The ShoreTel Converged Conference Solution and the ShoreTel Contact Center Solution are managed separately with their own management systems.

The ***ShoreTel 8*** system provides automated software distribution for all components on the system. When you add a new ShoreGear voice switch to the system, it is automatically upgraded to the current software release by the ShoreWare server. Existing ShoreGear voice switches will download the current software when you reboot the switch (see Section 4.2.1 on page 50). The Headquarters server does not upgrade distributed servers. Distributed servers must be upgraded independently.

When you add a new user to the system, the user receives an email message containing a URL from which desktop call control and unified messaging applications can be downloaded and installed.

For software upgrades at the Headquarters site, you simply install the new software on the ShoreWare servers. Users are notified of the new software release and are automatically prompted to upgrade their software, if an upgrade is mandatory.

The ***ShoreTel 8*** management software also provides a complete suite of maintenance tools that enable you to monitor and change the status of components on the system. The system can be configured with event filters that automatically generate an email message if an error occurs on the system.

2.3 ShoreTel System Communications

ShoreTel system communications can be divided into four basic communication types:

- Call Control
- Configuration
- TAPI
- Media

The communication streams and the protocols that support them are explained in the following sections.

2.3.1 Call Control

ShoreTel uses two protocols to process and manage calls:

- Media Gateway Control Protocol (MGCP)
- An enhanced version of Session Initiation Protocol (SIP)

Media Gateway Control Protocol (MGCP) is used between IP phones (and other IP endpoints) and ShoreGear switches. MGCP manages the setup and teardown of media streams and some basic phone operations.

Figure 2-3 shows where SIP and MGCP are used in a ShoreTel system.

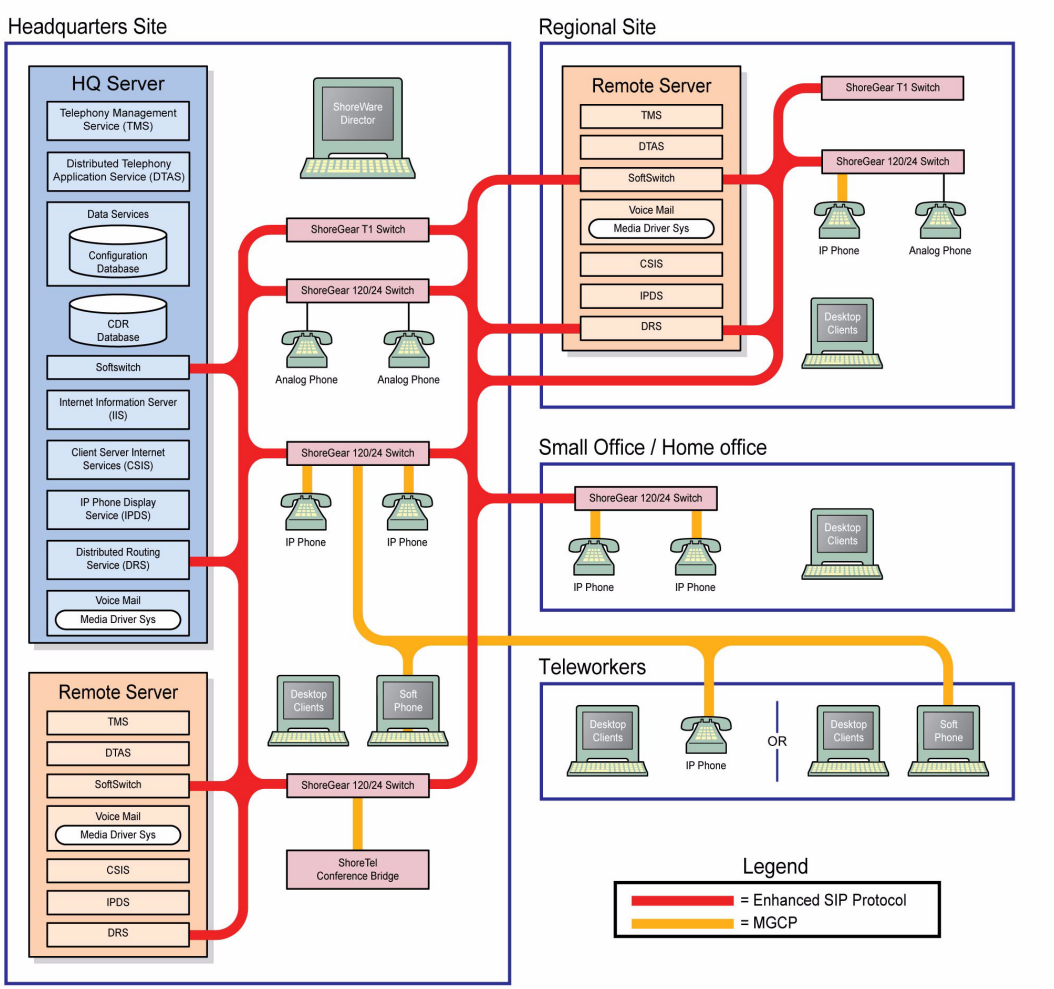

Figure 2-3 SIP and MGCP in a ShoreTel System

Call control between ShoreTel switches is based on the emerging Session Initiation Protocol (SIP), an application-layer protocol defined by IETF for voice-over-IP applications. Independent of the packet level, SIP establishes, modifies, or terminates sessions without respect to media content. Because of its extensibility and advanced integration capabilities, SIP is considered the next-generation protocol standard for real-time communications.

2.3.1.1 ShoreTel's Enhanced SIP Call Control

In ShoreTel's implementation of SIP call control, functions are split among the following software modules:

- User Agent
- Location Service
- Local Call Routing Service
- Admission Control Service
- Bandwidth Manager

SIP architecture deploys a peer-to-peer model in which endpoints can function either as clients or servers.

User Agents

User agent objects represent call endpoints—an extension or a trunk. Each user agent is addressable by a SIP URL.

For extensions, the URL syntax is:

sip:nnn@ip_addr:5441, where

nnn = extension number
ip_addr = ip address
5441 = UDP port number used by ShoreTel Call Control

For trunks, the URL syntax is:

sip:TGrp_xxxpyy@ip_addr:5441, where

xxx = trunk group number
yy = port number
5441 = UDP port number used by ShoreTel Call Control

In ShoreTel's call control protocol, user agents representing endpoints on an IP network operate as peers, functioning as clients when initiating requests, and as servers when responding to requests.

Location Service

Endpoint location exchange is performed via ShoreTel's proprietary Location Service Protocol (LSP). When switches first connect, they exchange all known SIP URLs. Afterwards, only configuration updates are transmitted.

LSP is based on UDP. The service relies on keep-alive pings (sent every 30 seconds) to detect dead switches.

Admission Control Service

Admission Control Service instructs Bandwidth Manager to reserve bandwidth for intersite calls. If a request is successful, updates are sent to Bandwidth Managers running on other switches at the same site.

Bandwidth Manager

A distributed Bandwidth Manager keeps track of intersite bandwidth use. A Bandwidth Manager runs on each ShoreGear switch.

ShoreGear switches reserve bandwidth from the Bandwidth Manager via the ShoreTel Bandwidth Reservation Protocol (BRP).

Figure 2-3 shows a hypothetical system with the call control protocols illustrated in simplified form.

2.3.1.2 Media Gateway Control Protocol

IP phones and other IP endpoints communicate with ShoreGear switches via MGCP, a device control protocol. The relationship between the switch (call manager) and the phone (gateway) follows a master–slave model.

MGCP, an industry-standard protocol, is used to:

- Deliver information to the IP phone display
- Set up and tear down media streams
- Report phone events such as key presses, on-hook, and off-hook

Figure 2-3 shows a hypothetical system with the call control protocols illustrated in simplified form.

2.3.2 Configuration

ShoreTel maintains a configuration database with all the static and dynamic system configuration data. Any modifications made to the configuration database are broadcast to other system components, such as the server applications and TMS.

The database is accessed and updated via Microsoft's Distributed Component Object Model (DCOM) protocol. ShoreTel also uses DCOM to send call information to the Call Detail Report (CDR) database, which is in Crystal Reports format.

TMS uses Network Call Control (NCC) to send each switch its configuration information. The ShoreGear switches that are connected to the network (via LAN/WAN) interact with the TMS using the NCC Client interface.

Figure 2-4 shows a hypothetical system with DCOM communication flows.

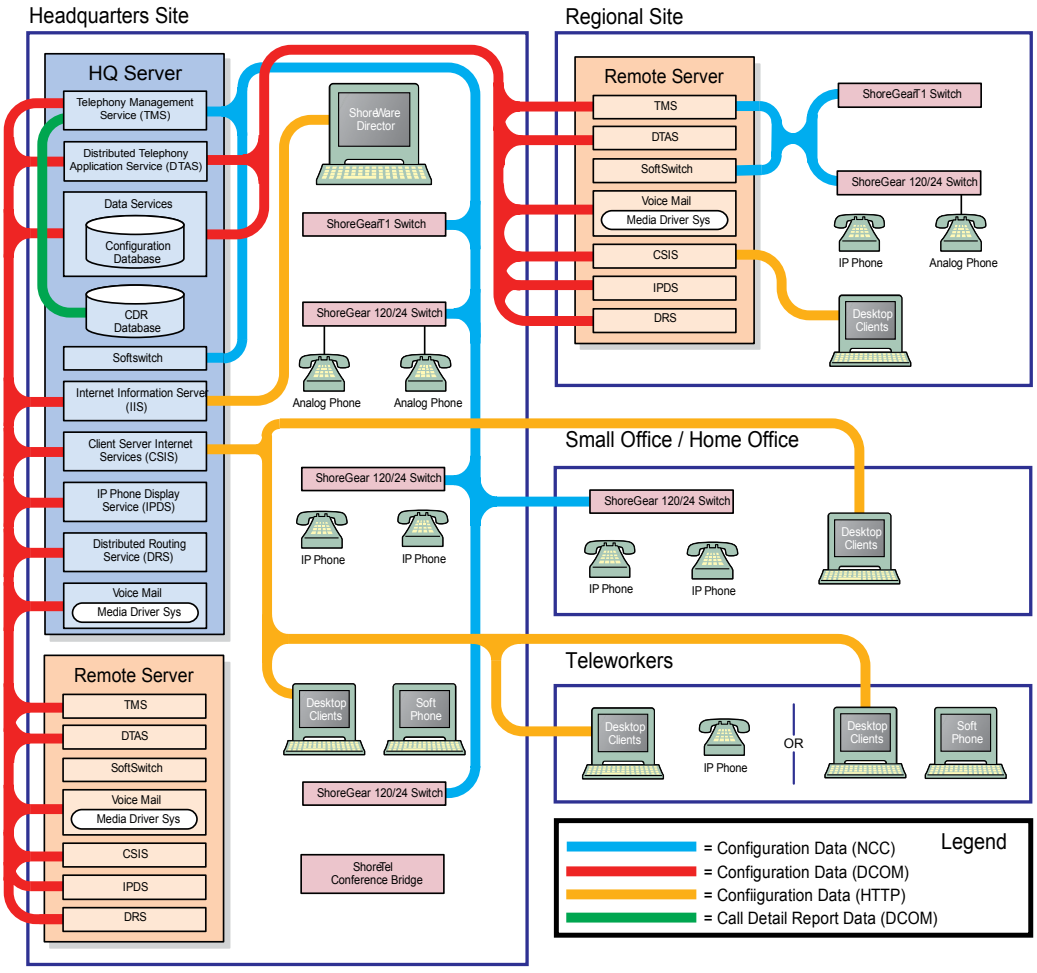

Figure 2-4 DCOM Protocol in a ShoreTel System

2.3.3 TAPI

All ShoreTel applications, including Workgroups, Voice Mail, and Account Code Collection, communicate via TAPI to other system components. All applications that need to interact with distributed call control do so via TAPI. Applications use TAPI to communicate call control information to TMS, and TMS communicates this information to all other system components as needed.

Figure 2-5 shows how the ShoreTel system uses NCC and RPC to pass TAPI information in the system.

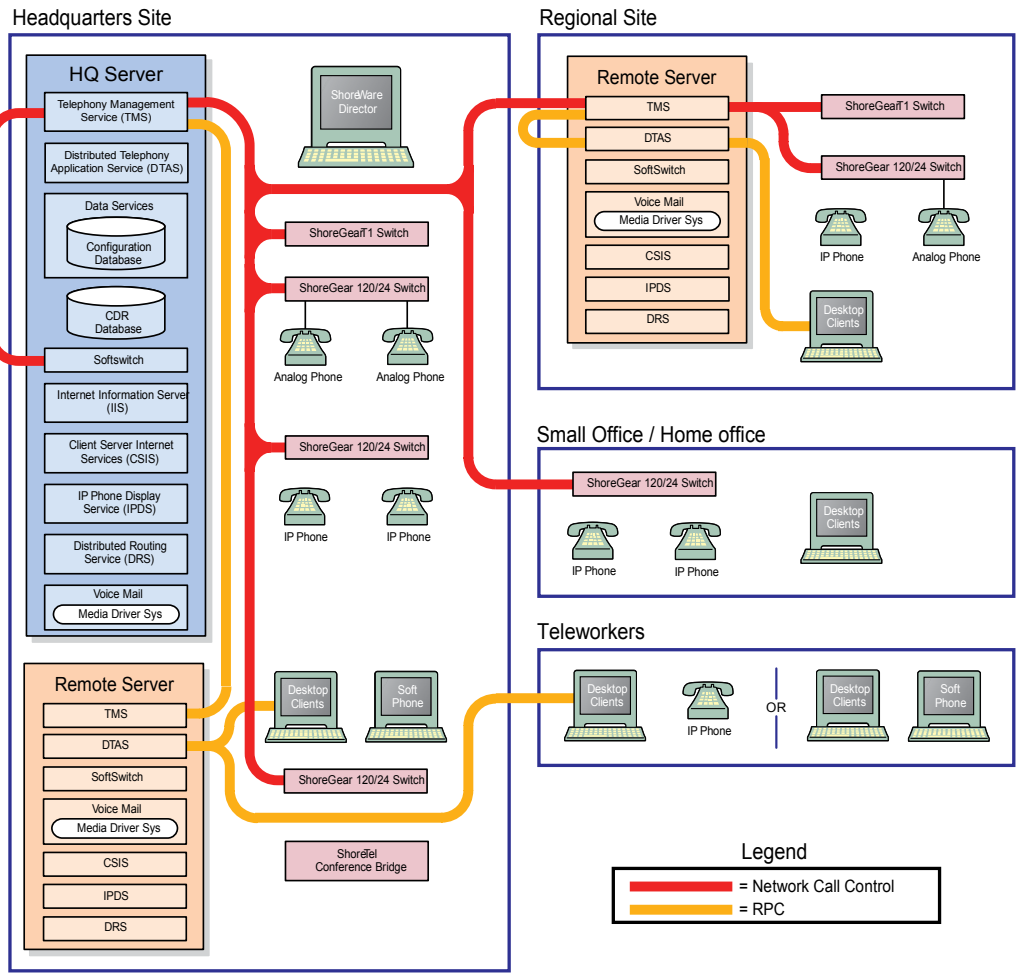

Figure 2-5 NCC and RPC Communications in a ShoreTel System

For example, whenever a user dials a number, the ShoreGear switch notifies TMS. TMS then presents that call information to the application via TAPI.

A service called the Distributed Telephony Application Service (DTAS) provides connectivity between applications and TMS instances. DTAS reads the system configuration so that it knows which extensions are controlled by which TMS instances. DTAS is responsible for routing call control and events between applications and the TMS instance responsible for a given extension. For extensions controlled by the local TMS instance, DTAS routes call control to the local TMS instance. For extensions controlled by a remote TMS instance. DTAS routes call control to the appropriate remote TMS instance.

DTAS makes the distributed TMS architecture transparent to applications and reduces the number of network connections that would be needed if every application had to connect to every TMS instance.

Switches are assigned to specific TMS servers through ShoreWare Director. Assignment of a switch to a TMS server is restricted to TMS servers at its own site, or if there is no TMS server at that site, to the nearest TMS servers in the site hierarchy above.

TAPI requests invoke ShoreTel's Remote TAPI Service Provider, which uses Remote Procedure Calls (RPC) to communicate with TMS. TMS uses Network Call Control to exchange commands and events with ShoreGear voice switches so that TMS can present extensions and trunks as TAPI lines to the applications.

2.3.4 Media

Media travels through the ShoreTel system using Real-Time Protocol (RTP). After call setup, media flows directly between IP phones via RTP. The ShoreGear switch is involved only when setting up or tearing down a call.

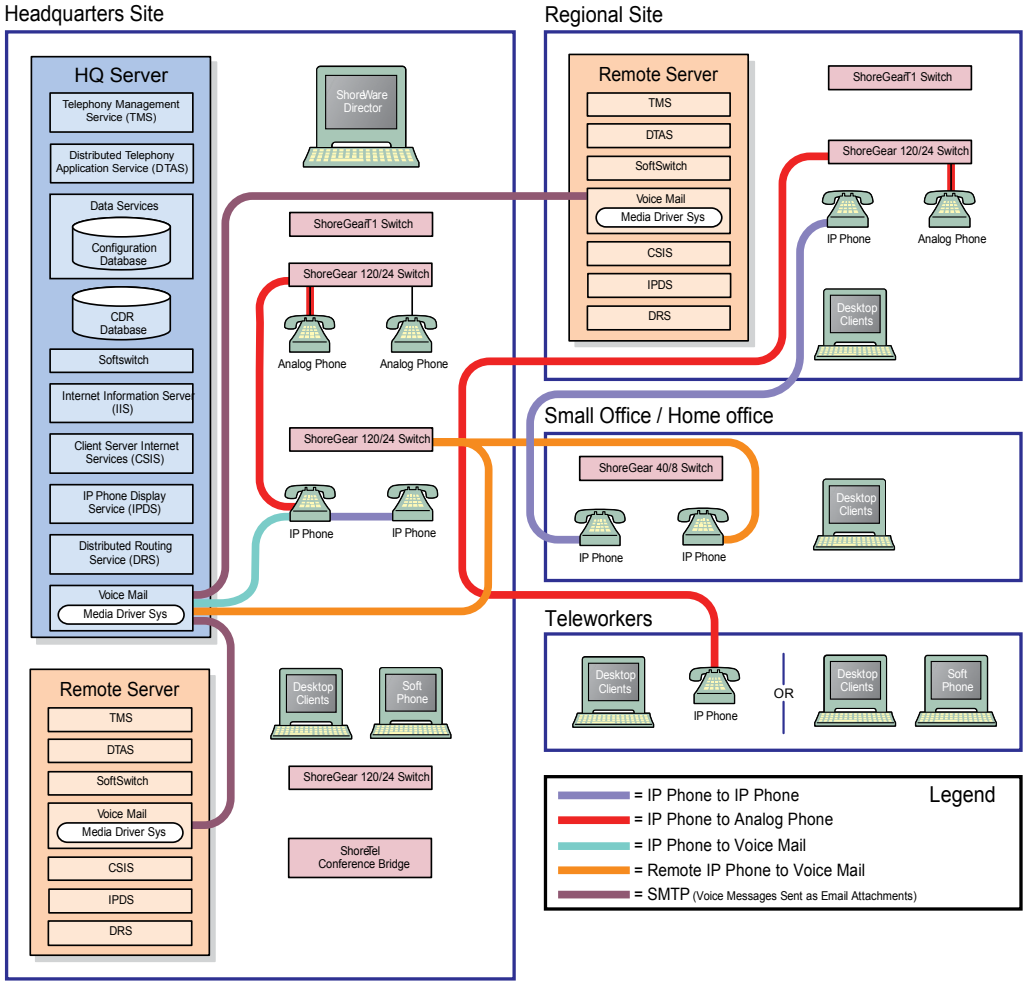

Figure 2-6 Media Traffic in a ShoreTel System

A voice mail message is normal RTP traffic, unless it is a recorded voice mail message moving from one server to another. Voice mail media streams conform to the G.711 codec. If a switch or IP phone is configured to use G.729 or ADPCM (for example, an intersite call), a media server proxy is used to transcode between G.729/ADPCM and G.711. Since the media server proxy is a switch resource, there are a limited number of G.729 proxies. If there are insufficient G.729 proxies, then ADPCM is used instead.

2.3.4.1 IP Phone to IP Phone

Media between IP phones or other IP endpoints such as SoftPhones, passes directly point to point.

2.3.4.2 IP Phone to Analog Phone

Analog phones depend on the ShoreGear switch to which they are connected. Media from IP endpoints must pass though the ShoreGear switch supporting the analog phone.

2.3.4.3 Analog Phone to Analog Phone

Media between analog phones passes though the switches supporting the analog phones.

2.3.4.4 Analog Phone to Voice Mail

Voice mail media from analog phones passes through the switch supporting the analog phone before going to voice mail via the server's media driver. When the analog phone is located on the same LAN as the host server, the ShoreGear voice switch connects to the server using a Mulaw codec. If the analog phone is connected via a WAN, and there are ShoreGear voice switch resources available, the ShoreGear voice switch will use an inter-site codec (G729 or ADPCM). If ShoreGear voice switch resources are not available, the call will revert to the Mulaw codec.

2.3.4.5 IP Phone to Voice Mail

Voice mail media from IP phones and endpoints goes directly to voice mail. IP phones at remote sites without a server send voice mail media to a ShoreGear switch, which then sends it to voice mail. This is done in order to use G.729 streams for voice mail across the WAN.

2.3.4.6 Voice Mail Between Servers

When recorded voice mail messages are transferred between servers, they are sent via SMTP.

2.4 System Reliability

System reliability is ensured at several levels, including:

2.4.1 Distributed Switch Control

The ShoreWare Telephony Management Service (TMS) runs on every ShoreWare distributed server, ensuring switch control even if there a WAN outage between the remote server and the headquarters site. Since multiple servers share the task of switch management, if a server fails, only the extensions it controls may be affected by a disruption in service.

Distributed TMS enables applications to handle calls on the switches at remote sites during a loss of network connectivity between the remote server site and the headquarters site. The co-located TMS's provide local control of switches and local control by applications such as the PCM client and IPDS via TAPI. Applications are able to provide all of the features they normally provide (during full WAN connectivity) for extensions on locally controlled switches. Monitoring and control of extensions on remotely controlled switches are still affected by WAN outages.

Distributed TMS also reduces the affects of a particular TMS/server outage to just those extensions controlled by that TMS instance.

Overall system scalability is increased with this feature because TMS instances control a subset of the switches in an entire system rather than all the switches in the system as in previous releases. Scalability is also increased because TMS instances handle a subset of PCM clients rather than all clients in the entire system.

2.4.1.1 WAN Outage

Distributed Telephony Application Service (DTAS) is responsible for routing call control and events between applications and the TMS instance responsible for a given extension.

When there is a loss of connectivity with the HQ database, DTAS continues to operate except that additions and deletions to the configuration will not been seen by IPDS. DTAS services involving the local TMS will be available. DTAS operations involving remote TMS instances not reachable because of the WAN outage will not be available.

Telephony operations involving locally controlled phones will be available. Monitoring of phones controlled by TMS's not reachable because of a WAN outage will not be available.

TMS continues to operate except that additions and deletions to the configuration will not been seen by TMS and not relayed to telephony clients. Telephony operations involving locally controlled phones will be available. If a WAN outage results in the loss of connectivity to one or more switches, telephony operations with those switches will be unavailable.

2.4.2 Embedded IP Phone Display Driver

Several tasks related to IP phone operation (models IP110/115/212k/230/530/560/560g) will be handled by the switch instead of the server. While previous releases placed control of many of the IP phone features at the server, this latest release shifts that control to the switch in order to enhance reliability and offer better uptime. Features that will be affected by this change include:

- Phone display
- Transferring a call
- Conference calls
- Placing calls on hold
- On-hook dialing
- Intercom
- Redial
- Pickup
- Park
- Unpark

Some features that would require writing to the database will continue to depend on the server being both operational and accessible. These features will not be handled by the switch but will continue to be provided by the server. The features that will continue to be provided by the server are:

- directory
- options
- speed dial (due to its reliance on the database)
- ability to change call handling modes
- wrap up
- monitoring extensions on other switches
- presence information for user serviced by other switches

No configuration is necessary to enable the new Embedded IP Phone Display Driver behavior. The change in functionality is transparent to the user.

2.4.3 Public Switched Telephone Network (PSTN) Failover

User extensions can be optionally configured to route extension-to extension calls to the public switched telephone network (PSTN) in the event that an IP connection is unavailable. Extension-to-extension calls are those a user makes to another site within a multi-site system, for example, a user in New York calling a co-worker at the company's San Francisco office. The IP connection may be unavailable due to lack of bandwidth or connectivity. The PSTN failover option must be explicitly enabled in the user' Class of Service and bypasses the caller's call permissions. For systems using Distributed Routing Service (DRS), destinations allowing PSTN failover handling return a contact list with a failover number. When a site does not have connectivity to DRS, users at other sites with DRS connectivity will be able to reach the users at that site using PSTN failover (as long as the destination site has trunks to accept the PSTN calls). This limitation has the biggest impact for small offices that do not have a local ShoreWare server.

2.4.4 Distributed CDR

In the event of a WAN outage, CDR data is stored for up to two hours on the distributed server. When WAN connectivity is restored, the stored data is forwarded to the Headquarters database. After two hours, the distributed server deletes the data and logs an error to the NT event log.

2.4.5 For More Information

Also refer to Chapter 6, starting on page 97 for more information about failover. For configuration details about PSTN failover configuration, CDR data, or IP phone configuration, see the ***ShoreTel 8 Administration Guide***.

2.5 Call Scenarios

To understand how the ShoreTel system processes calls, review the following call scenarios and flow charts.

2.5.1 On-hook Call from Personal Call Manager

Figure 2-7 shows the communication protocols and components participating in a call dialed from Personal Call Manager to a PSTN destination.

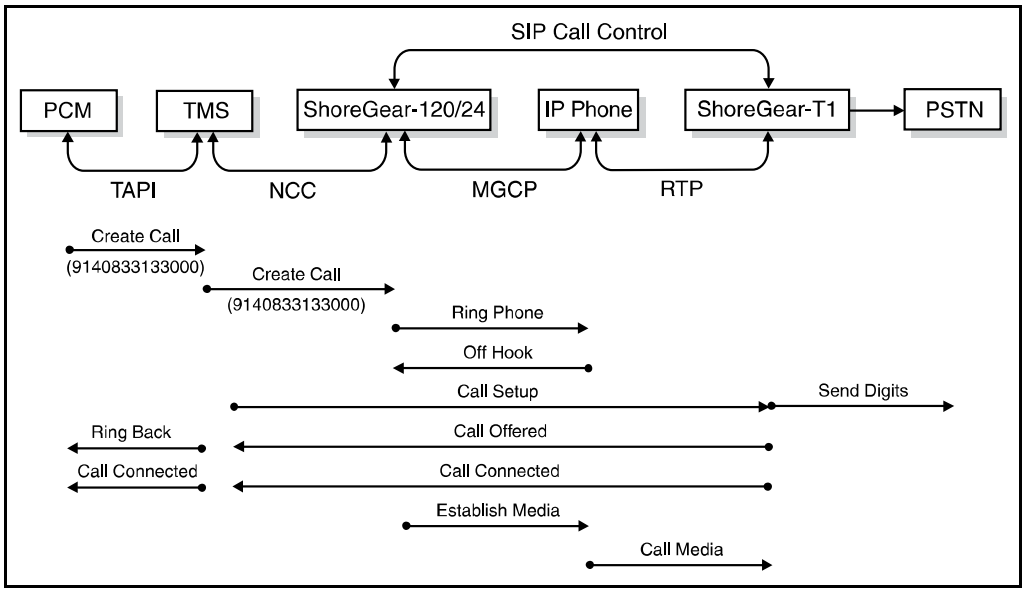

Figure 2-7 ShoreTel Communications for a Call from Personal Call Manager

2.5.2 Quick Dial Call from Personal Call Manager

Figure 2-8 shows how a call dialed from a user's Personal Call Manager Quick Dial is handled by the system.

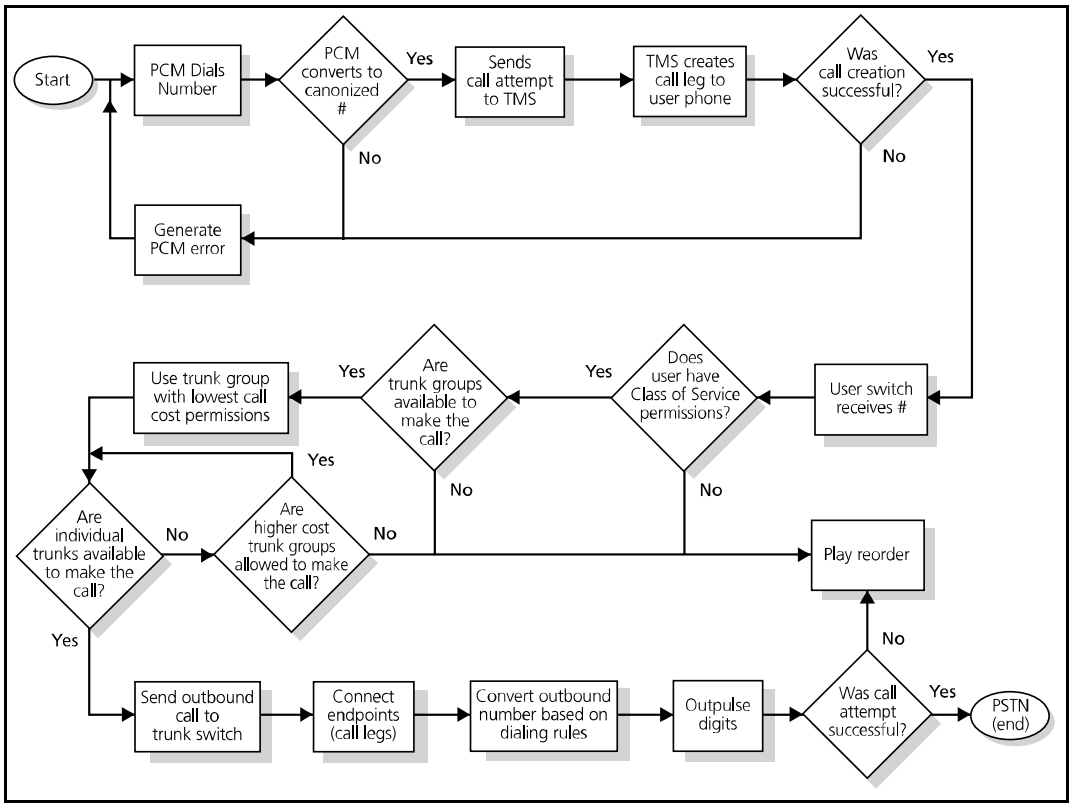

Figure 2-8 Call Flow for a Quick Dial Call from Personal Call Manager

2.5.3 Inbound Call from a Trunk

Figure 2-9 shows how an inbound call on a trunk is connected to its destination.

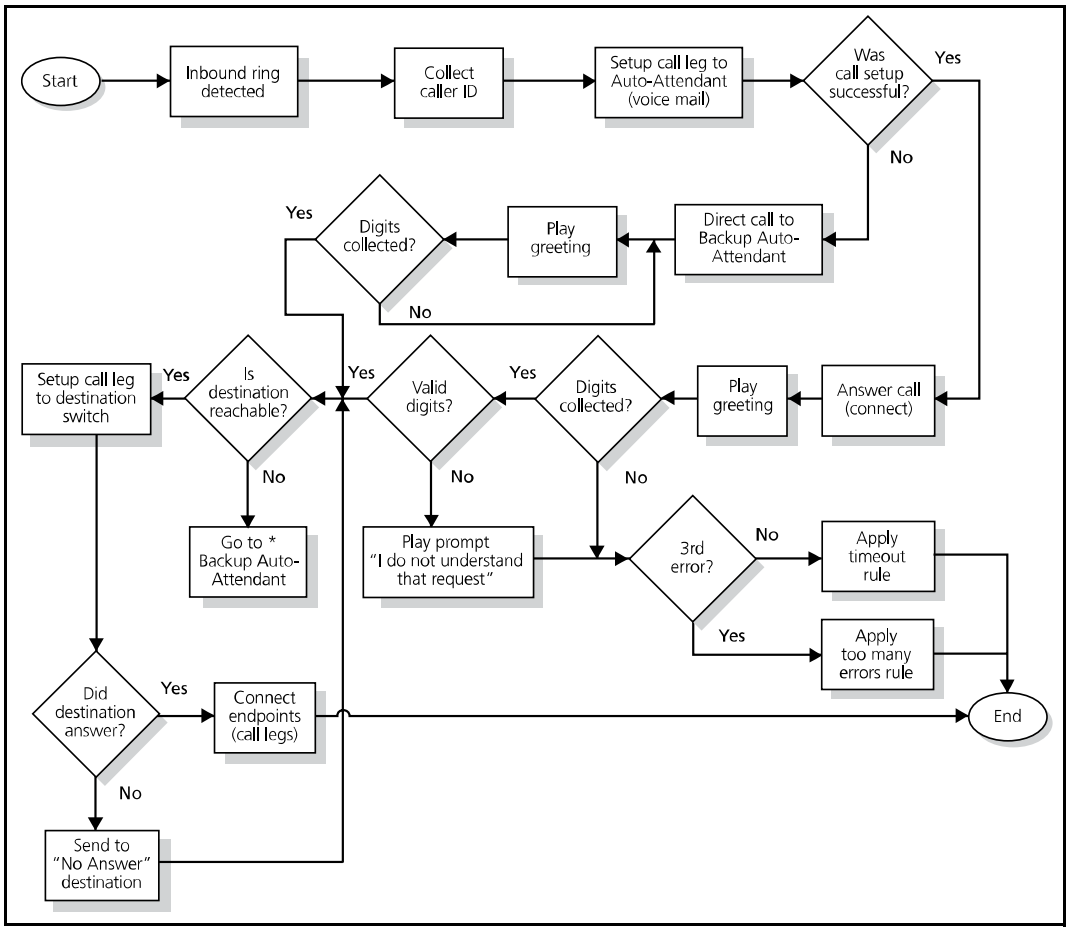

Figure 2-9 Call Flow for an Inbound Trunk Call

2.6 Reference

The following tables list the UDP and TCP ports used by ***ShoreTel 8*** processes.

2.6.1 TCP/IP Ports Used by the ShoreTel System

This section describes how ShoreTel system components interconnect via a TCP/IP network.

2.6.1.1 ShoreGear Voice Switch and ShoreWare Server Connections

Each ShoreGear voice switch exchanges information about the state of calls it is managing with the ShoreWare server. When a switch starts, it negotiates a connection to TMS using RPC. The source port used is dynamic and the destination port is negotiated with the ShoreWare server using the Sun RPC port mapper. The port mapper sends the request via TCP and UDP port 111. When the RPC port has been negotiated, the ShoreGear voice switch establishes a connection with the server using TCP ports in the 1024 to 65535 range. This connection persists until the Ethernet connection is lost, or either the switch or server is rebooted.

Each ShoreWare server uses a SoftSwitch to participate in the system's distributed call control. The SoftSwitch communicates with other ShoreGear voice switches using UDP ports 5440, 5441, 5442, 5443, 5445, and 5446. These ports are connected when the SoftSwitch is communicating with any other ShoreGear voice switch.

Switches and servers send and receive voice media using the RTP protocol on UDP port 5004. Media streams are established each time a connection between the server and switches is needed to send audio between the devices.

ShoreGear voice switches can be configured to boot using FTP as a boot source. This fallback method allows the switch to boot should its flash memory fail. When a switch is in boot from FTP mode, it downloads its operating system and call control software using FTP.

You can run switch diagnostics from the server using the ShoreTel tool ipbxctl. This tool runs a set of commands on the switch and sends the output to the server using TCP port 5555. This port is only used for the time needed to send the output.

Telnet connection to the ShoreGear voice switches is via the standard TCP port 23.

DHCP is used to set the IP parameters of the switch at boot up.

The following table illustrates the ports used for server to switch and switch to server communications.

Protocol	Transport	Source Port	Destination Port	Description
RPC	TCP		111	Used by SunRPC Port Mapper to negotiate TCP/UDP ports for TMS-to-switch communications.
RPC	UDP		111	Used by SunRPC Port Mapper to negotiate TCP/UDP ports for TMS-to-switch communications.
RPC	TCP	Dynamic	1024 - 65535	Used by Network Call Control to pass call status and control messages from the switch to the TMS. Ports are negotiated at startup and whenever the network connection is established.
RTP	UDP	Dynamic	5004	Used to transport media steams to and from the ShoreGear voice switches, ShoreWare server, IP phones, and conference bridge ports.
Call Control	UDP	5440	5440	Location Service Protocol
Call Control	UDP	5441	5441	Used by ShoreTel Call Control protocol to send call control information between the ShoreGear voice switch and the server SoftSwitch.
Call Control	UDP	5442	5442	Used by Distributed Routing Service to route inter-site calls.
Call Control	UDP	5443	5443	Used by the Bandwidth Manager to communicate the bandwidth currently in use on the ShoreGear voice switch.
Call Control	UDP	5445	5445	Used by the Admission Control Manager.
Call Control	UDP	5446	5446	Used by Distributed Routing Service to route inter-site calls.
	TCP	Dynamic	5555	Used to pass output back to the server when commands are sent to the switch using the ipbxctl diagnostic tool on the ShoreWare server.

Table 2-1 Server to Switch and Switch to Server Communication Ports

Protocol	Transport	Source Port	Destination Port	Description
FTP	TCP	Dynamic	21	Used to download switch software when the switch is configured to boot from FTP.
Telnet	TCP	Dynamic	23	Used to connect a Telnet session to a ShoreGear voice switch.
DHCP	UDP	68	68	
BootP	UDP	68	68	Used to assign IP parameters to the switch when configured to use DHCP

Table 2-1 Server to Switch and Switch to Server Communication Ports

2.6.1.2 ShoreGear Voice Switch to ShoreGear Voice Switch Connections

ShoreGear voice switches provide the distributed call control within the ShoreTel system. Each ShoreGear voice switch participates in the system's distributed call control. The switches communicate with other ShoreGear voice switches using UDP ports 5440, 5441, 5442, 5443, 5445, and 5446.

ShoreGear voice switches send and receive voice media using the RTP protocol on UDP port 5004. Media streams are established each time a connection between the server and voice switches is needed to send audio between the devices.

The following table illustrates the ports used for switch to switch connections.

Protocol	Transport	Source Port	Destination Port	Description
RTP	UDP	Dynamic	5004	Used to transport media steams to and from the ShoreGear voice switches, ShoreWare server, IP phones, and conference bridge ports.
Call Control	UDP	5440	5440	Location Service Protocol
Call Control	UDP	5441	5441	Used by ShoreTel Call Control protocol to send call control information between the ShoreGear voice switch and the server SoftSwitch.
Call Control	UDP	5443	5443	Used by the Bandwidth Manager to communicate the bandwidth currently in use on the ShoreGear voice switch.
Call Control	UDP	5445	5445	Used by the Admission Control Manager.

Table 2-2 Switch to Switch Communication Ports

2.6.1.3 IP Phone to ShoreWare Server Connections

The IP phones participate in the distributed call control by communicating to the ShoreGear voice switches using MGCP. Each IP phone is assigned a call manager switch. The phone sends and receives call control information to the call manager switch using MGCP. MGCP uses UDP ports 2427 and 2727. These ports are established when the phone is active.

The switches and servers send and receive voice media using the RTP protocol on UDP port 5004. Media streams are established each time a connection between IP phones and switches or servers is needed to send audio between the devices.

The IP phones download firmware and configuration information from the ShoreWare servers using FTP to transport the files between the switch and the phone. FTP transport is via TCP port 21. The phone checks for software and configuration updates each time it is booted. If it detects the need for an update this happens automatically.

Telnet is used to establish a terminal session with IP phones.

DHCP is used to set the IP parameters of the IP phone at bootup.

The following table illustrates the ports used for IP phone to ShoreGear voice switch and server connections.

Protocol	Transport	Source Port	Destination Port	Description
MGCP	UDP	Dynamic	2427	MGCP call control and status from the IP phone.
MGCP	UDP	2727	2727	MGCP call control and status from the ShoreGear voice switch.
RTP	UDP	Dynamic	5004	Used to transport media steams to and from the ShoreGear voice switches, ShoreWare server, IP phones, and conference bridge ports.
FTP	TCP	Dynamic	21	Used to load firmware and configuration information from the ShoreWare server.
Telnet	TCP	Dynamic	23	Used to connect a Telnet session to a IP phone.
DHCP	UDP			Used to assign IP parameters to the switch when configured to use DHCP.

Table 2-3 IP Phone to Switch and Server Communication Ports

2.6.1.4 ShoreWare Server to ShoreWare Server

Each ShoreWare server uses a SoftSwitch to participate in the system's distributed call control. The SoftSwitch communicates with other ShoreGear switches using UDP ports 5440, 5441, 5442, 5443, 5445, and 5446. These ports are connected when the SoftSwitch is communicating with any other ShoreGear voice switch.

When a voice mail message is left for a user on a server where their voice mail box does not reside, it is sent to the appropriate voice mail server using SMTP. This is done using TCP port 25 and is established on an as needed basis.

The following table illustrates the ports used for server to server connections.

Protocol	Transport	Source Port	Destination Port	Description
RPC	TCP	Dynamic	1024 - 65535	Used by Network Call Control to pass call status and control messages from the switch to the server TMS process. Ports are negotiated at startup and whenever the network connection is established.
Call Control	UDP	5440	5440	Location Service Protocol
Call Control	UDP	5441	5441	Used by ShoreTel Call Control protocol to send call control information between the ShoreGear voice switch and the server SoftSwitch.
Call Control	UDP	5442	5442	Used by Distributed Routing Service to route inter-site calls.
Call Control	UDP	5443	5443	Used by the Bandwidth Manager to communicate the bandwidth currently in use on the ShoreGear voice switch.

Table 2-4 Server to Server Communication Ports

Protocol	Transport	Source Port	Destination Port	Description
Call Control	UDP	5445	5445	Used by the Admission Control Manager.
Call Control	UDP	5446	5446	Used by Distributed Routing Service to route inter-site calls.
SMTP	TCP	Dynamic	25	Used to send voice mail messages received on the source server to the server where the users voice mail box resides.

Table 2-4 Server to Server Communication Ports

2.6.1.5 ShoreWare Server to ShoreWare Director Client

ShoreWare Director uses an Internet Explorer browser to connect to the ShoreWare server using standard HTTP protocol. This connection used for configuration and monitoring of the system and the port is established for the duration of the session.

FTP is used to transport prompt files when they are being recorded or listened to using ShoreWare Director.

The following table illustrates the ports used for server to ShoreWare Director connections.

Protocol	Transport	Source Port	Destination Port	Description
HTTP	TCP	Dynamic	80	Used by ShoreWare Director clients to communicate to the ShoreWare Director Web server running on the ShoreWare server.
FTP	TCP	Dynamic	21	Used to transport Auto Attendant, Workgroup, Route Point prompts, and greeting recording and reviewing.

Table 2-5 Server to ShoreWare Director Communication Ports

2.6.1.6 ShoreWare Server to ShoreWare Personal Call Manager

The Personal Call Manager allows a user to manage personal options such as call handling modes, notifications, and other personal parameters of the ShoreTel system. Information is sent and received to the ShoreWare server using HTTP on port 5440 This port is established each time the PCM is launched on a desktop.

The server sends voice mail notifications and attachments to the voice mail viewer and Outlook using HTTP port 5440. The PCM sends call control requests to the ShoreWare server using the winsock protocol and receives call control information and status via RPC. The RPC connection is established by negotiating a port between 1024-65535 with the server. The RPC port is established for the duration of the connection and is reset each time the PCM is launched or the Ethernet connection is lost and restored.

The following table illustrates the ports used for server to PCM connections.

Protocol	Transport	Source Port	Destination Port	Description
HTTP	TCP	Dynamic	5440	Used by CSIS to send and receive voice mail messages between the server and the client. Used to send and receive configuration information.
Winsock				Used to send call control from the PCM to the ShoreWare server.
RPC	TCP	Dynamic	1024 - 65535	Used to receive call control status from the server.

Table 2-6 Server to Call Manager Communication Ports

CHAPTER 3

ShoreWare Servers

3.1 Overview

The ShoreTel voice over IP telephony solution is a suite of software modules, applications, and services running on a ShoreWare server. Every ShoreTel system has a main server called the Headquarters server. In a single-site system, the Headquarters server may be the only ShoreWare server. More complex systems may include distributed servers to add reliability for applications and switches on remote sites or to support distributed applications. The Headquarters server remains the main server and must be available to interact with the distributed servers for full system functionality.

3.1.1 Headquarters Server

The Headquarters server is the main ShoreWare server and hosts the voice applications platform and the management Web site, as well as the integrated voice applications. Typically, the Headquarters ShoreWare server is located at the largest location, containing the majority of users.

The Headquarters server hosts a SoftSwitch that provides extensions for the Auto-Attendant, Workgroups, and virtual users.

This version of ShoreTel software was tested and certified on Windows Server 2003 (Enterprise or Standard Editions only) with and without SP1, and Windows Server 2003, Release 2.

3.1.2 Remote Servers

The ShoreTel system also supports remote servers. Remote servers provide increased system reliability by duplicating some key services at remote sites. Each remote server has an instance of TMS that only connects to and manages the SoftSwitch. The SoftSwitch provides extensions for use by the local Auto-Attendant, Workgroups, and virtual users.

ShoreTel remote servers can also be configured to support specific distributed voice applications such voice mail. Remote servers only have TAPI access to the local SoftSwitch. The distributed TMS maintains a copy of the configuration database that allows it to provide call control and voice mail service during the outage. Each remote server manages its own SoftSwitch, as well as ShoreGear switches assigned to it.

Remote servers are valuable for the following purposes:

- They reduce bandwidth because local users' calls to voice mail are answered by the local voice mail application and do not pass across the WAN.
- They increase system scale by extending the unified messaging and desktop call control services to additional users of the applications.
- They increase system scale and reliability by providing distributed switch management, call control services, and unified messaging.

Call control is provided by Headquarters and remote servers even if full network connectivity is unavailable. However, calls to unreachable endpoints cannot be made, and call detail recording requires Headquarters communication. To add reliability to your remote server, consider using redundant network paths to the Headquarters server.

The following sections provide more detail on the communications, services, and applications.

3.1.3 Configuration Communications

ShoreTel system processes use Microsoft Distributed Component Object Model (DCOM) objects to share information from the configuration database among themselves and to write configuration information to the database. Static configuration parameters are written to the database by ShoreWare Director and system components access the database to read/write current state information. User configuration options are written to the database from Personal Call Manager, the telephone interface (voice mail options), and Web Access. Director is accessed via a Web browser,

The service ShoreTel-ZIN, running on the Headquarters server, manages these DCOM communications for TMS. There is a single instance of the ShoreWare database on the Headquarters server.

Each ShoreTel service on a distributed server caches its own copy of the configuration database in internal data structures. When a distributed server loses connection to the Headquarters server, changes made to the Headquarters configuration database are no longer received by the distributed server. However, services continue to function with the most recent configuration data until connectivity is restored. When the connection is restored, the distributed server automatically receives and incorporates any changes made to the Headquarters database during the outage.

If a distributed server restarts without a connection to the Headquarters database, then ShoreTel services are started but are not functional. When the network connection is restored, the configuration is retrieved and again cached by each service and services become functional.

ShoreWare client applications, such as Personal Call Manager, use CSIS for data handling. The CSIS server communicates with ShoreWare clients via HTTP. ShoreWare Director accesses the configuration database though IIS.

You can use the Component Service Manager to view DCOM objects installed by the ShoreWare software. Component Service Manager is located in the Administrative Tools folder available from the Windows Start menu.

Do not change any permission or security settings for ShoreWare components.

Features accessible from the voice mail phone interface that require write access to the database, such as Office Anywhere and Call Handling Mode changes, are not supported during an outage.

The block diagram below illustrates how ShoreWare services use Distributed Component Object Model (DCOM) to access the configuration database, and thus maintain the system status.

3.1.3.1 Internet Information Service

The ShoreWare server uses IIS to implement ShoreWare Director's browser-based interface. You can use the Internet Services Manager to view the configuration of the ShoreWare Director Web site. ShoreTel installs the site configuration using the installation program. Changing the default configuration installed by ShoreTel may cause the Director Web site or other system components to fail.

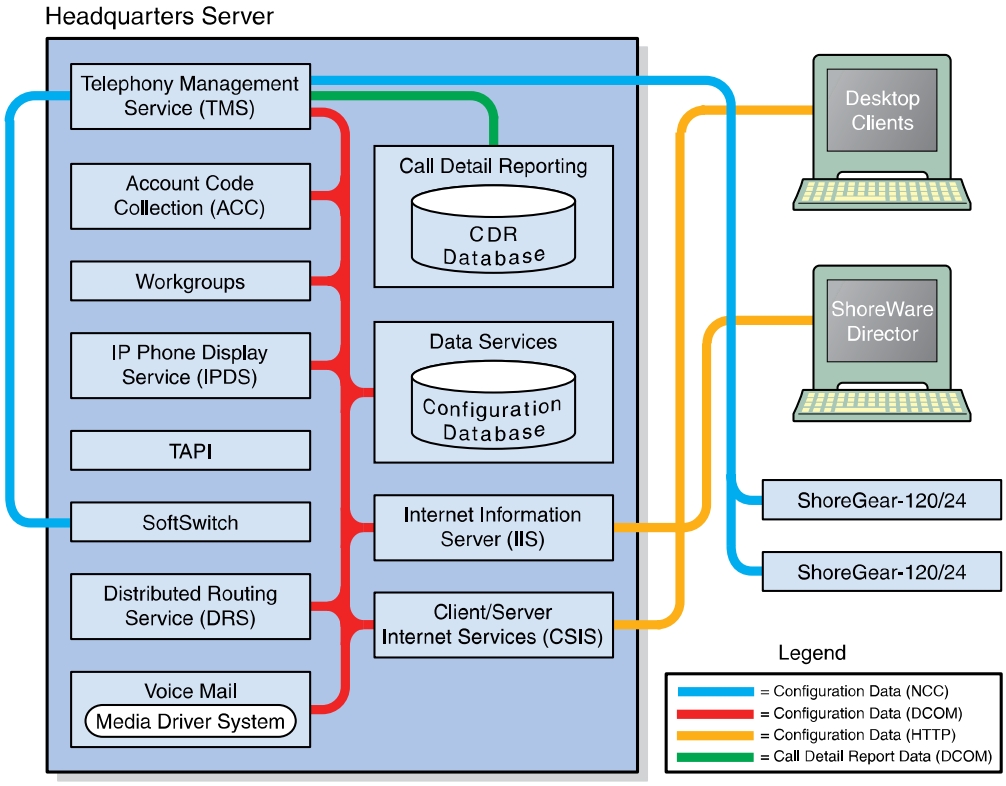

Figure 3-1 ShoreWare Server Database Communications

WARNING If the anonymous access user gets modified or its password is changed, the TMS service will not start. Changing the properties of this user may mean you have to rebuild the server to recover.

FTP Services

Both the Headquarters and remote servers make an FTP service available for fall-back use by ShoreGear switches. While this does not have to be active on a continuous basis, the FTP site needs to be active for the fallback capability to work. ShoreTel recommends that the FTP site always be available.

The ShoreWare server also uses the FTP service to transfer prompts between applications.

The IP phones use the FTP server to download configuration information and the application program when they boot. They will download these files from the server that is controlling the switch managing the IP phone.

To view the FTP site properties, use the Internet Services Manager. Anonymous FTP access must be maintained in order for all ShoreTel applications to use it.

SMTP Services

The ShoreTel software uses SMTP to send email notifications (for example, when new client software is available for installation). The voice mail system uses SMTP to transport composed messages between the distributed servers. SMTP services are also required by the Event Notification feature.

The ShoreTel installer does not make any specific configurations to the SMTP service. The applications deposit outbound email on the server for forwarding elsewhere.

For proper operation of the ShoreTel services, the hosting enterprise must have an email server configured to accept and forward SMTP mail. This is usually the exchange server or primary email server for the company.

Client/Server Internet Services

CSIS is a ShoreTel proprietary protocol that uses HTTP messages to communicate between client PCs and Shoreware servers. The CSIS protocol communicates configuration updates such as call handling mode settings and Outlook integration. The CSIS client holds open a pending HTTP request in order to receive notifications from the CSIS server. Network devices, such as firewalls and proxies, must not automatically close these pending requests.

3.1.3.2 IP Phone Services

IP phones in a ShoreTel system rely on two services running on the Headquarters server and distributed servers:

- IP Phone Configuration Service (IPCS)—Runs on HQ server only.
- IP Phone Display Service (IPDS)—Runs on all servers.

The IP Phone Configuration Service (IPCS) manages the IP phone configuration process, including configuration file downloads and the database updates.

IP Phone Display Service (IPDS) controls any actions by the IP phone display not controlled by the device's firmware or switches.

3.1.3.3 Event Watch

Event Watch monitors the NT Event Log and delivers email notifications of selected events. Event notifications are configured from the Events Filter page in ShoreWare Director. For more information, see the ***ShoreTel 8 Administration Guide***.

3.1.3.4 Call Detail Reporting

TMS use DCOM to write call data to the Call Detail Report database. The ShoreTel system tracks all call activity and generates call detail records into a database as well as into a text file on the ShoreWare server. The call detail records are used to generate CDR reports.

For more information on Call Detail Reports, see the ***ShoreTel 8 Administration Guide***.

3.1.4 Call Control Communications

The ShoreWare server provides call control for server applications and for Distributed Routing Service (DRS).

3.1.4.1 TAPI

The ShoreWare server and its client applications use Telephony Application Programming Interface (TAPI) to direct applications and provide the system with call control.

The TMS application service acts as the ShoreTel TAPI service provider and is responsible for managing the system's TAPI lines and routing information to other applications.

When TMS starts up, it creates a TAPI line device for each endpoint in the system. Access to these TAPI lines is provided through ShoreTel Remote TAPI Service Provider (RPCTSP.tsp). This is installed on each of the systems that run ShoreWare clients, (such as Call Manager), ShoreWare server (for example, voice mail servers), and distributed servers. Every application that has access to these TAPI lines receives new calls, call state information, and line device information from TMS via RPCTSP.tsp.

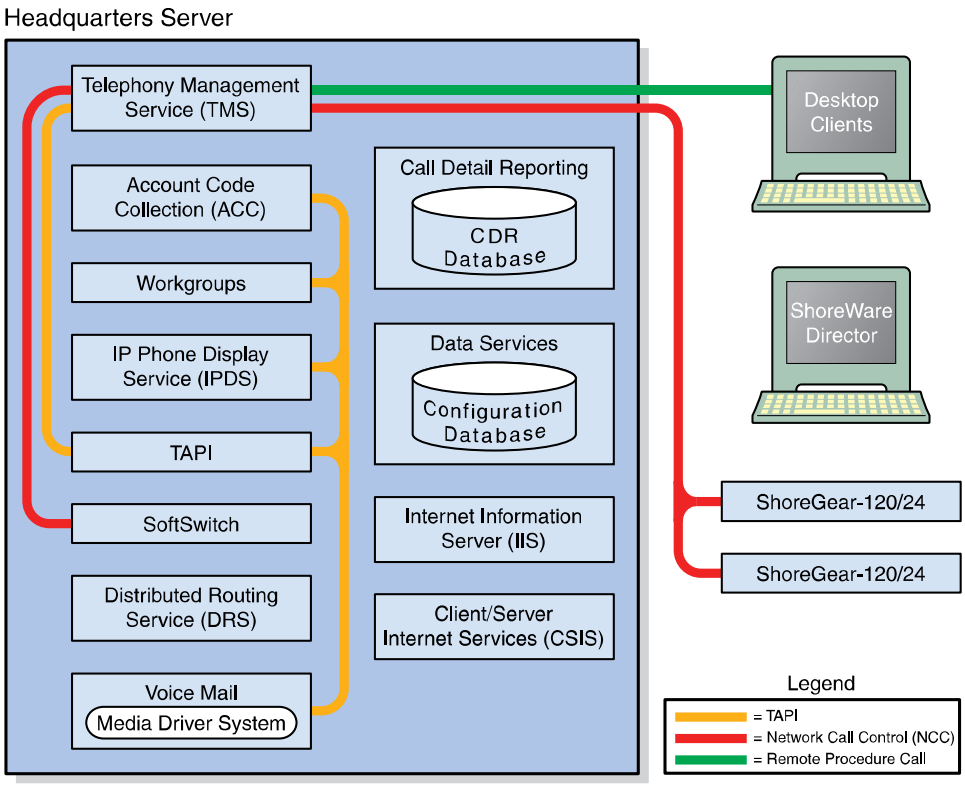

Figure 3-2 ShoreWare Server TAPI Communications

The Telephony Management Service (TMS) uses NCC to communicate with the ShoreGear switches, and a combination of RPC and Windows sockets (Winsock) to communicate with a remote TAPI service provider.

To view the properties of the ShoreTel Remote TAPI Service Provider, open the Phone and Modem Options tab in the Windows Control Panel.

Never modify the TAPI properties of ShoreTel Remote TAPI Service Provider. Modified TAPI properties can cause ShoreTel clients or applications to fail.

3.1.4.2 Distributed Routing Service

DRS on the server provides routing information when switches are unable to connect a call to through the local path. ShoreTel's enhanced SIP protocol is used for the switch to DRS communications (see Figure 3-3).

3.1.5 Media Communications

Media, from the perspective of the server, is connecting voice mail and the Auto-Attendant to switches and endpoints via the media driver. Media travels through the ShoreTel system using Real-Time Protocol (RTP).

A voice mail message is normal RTP traffic, unless it is a recorded voice mail message moving from one server to another. Voice mail media streams conform to the G.711 codec. If a switch or IP phone is configured to use G.729 or ADPCM (e.g. intersite call), a media

server proxy is used to transcode between G.729/ADPCM and G.711. Since the media server proxy is a switch resource, there are a limited number of G.729 proxies. If there are insufficient G.729 proxies, then ADPCM is used instead.

Figure 3-3 shows the switch-to-switch call control and media communications flows.

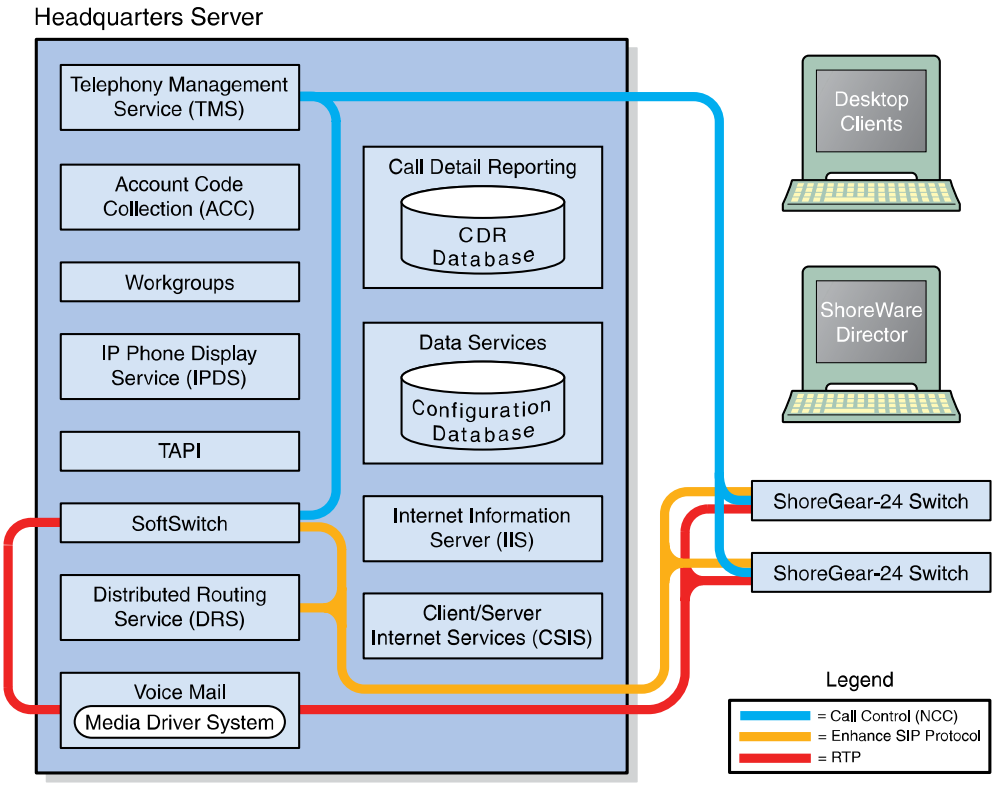

Figure 3-3 ShoreWare Server Call Control and Media Communications

For more information on ShoreTel's SIP-based call control, see Section 2.3.1.1 on page 8.

3.1.6 Integrated Server Applications

There are several integrated TAPI applications running on the server. These applications use TAPI to send and receive call control information, and can also manipulate calls. These applications also use ZIN Manager and DCOM to access and update the configuration database.

3.1.6.1 Voice Mail

Voice mail is a TAPI application that supports 254 simultaneous voice mail or Auto-Attendant connections. The voice mail system uses SMTP to transport composed messages between the distributed servers. Media streams to voice mail use RTP packets to send media.

Voice messages are stored on the server's hard drive in the VMS MESSAGE subdirectory of the Shoreline Data directory. Voice mail messages are stored as .wav files. To help you calculate storage requirements, one hour of messages requires approximately 28.8 MB of disk space.

The voice mail application consists of the following services: Port Manager and Mail Server. The Port Manager uses TAPI to interact with TMS. The ShoreTel system also supports linking to legacy voice mail systems using AMIS and SMDI protocols.

Distributed Voice Mail

Should the Headquarters server lose network connectivity, the distributed voice mail application allows SoftSwitches on distributed ShoreWare servers to continue handling voice mail calls and access the Auto-Attendant.

During an outage, users can only access voice mail though their phone interface. If users were running PCM at the time of the outage, they can still compose and playback messages. Users who were not running PCM at the time of the outage, or who restart PCM, will not be able to access their voice mail boxes until connectivity is restored.

Voice mail messages to mail boxes hosted at other sites will be stored and forwarded when connectivity to the destination voice mail service is restored.

3.1.6.2 Workgroups

Workgroups is an integrated Automated Call Distribution (ACD) application. Running on the Headquarters server, this TAPI application is responsible for routing and queueing calls directed to ShoreTel workgroups.

In the larger enterprise, there may be small- to medium-sized groups working together as a contact center. The ShoreTel Contact Center Solution is a server-based ACD and reporting package that includes the ability to queue and distribute calls, and provide agent and supervisor functions, as well as deliver reports on the call center activity.

3.1.6.3 Account Code Collection Service

The Account Code Collection Service (ACC) is a TAPI application running on the Headquarters server. When it is enabled, it allows account codes to be required or optional for outbound calls. When a restricted PSTN call is attempted, and account code collection is enabled, the ShoreGear switch redirects the call to ACC.

Account Code Collection Service is responsible for:

- Prompting the user for the account code
- Collecting and validating the account code
- Attaching the account code to the call for reporting purposes
- Performing a blind transfer to the external number

If the Headquarters server is down, or ACC is not available, the call is directed to the Backup Auto-Attendant.

TMS provides the following information to ACC:

- Dialed number
- User group
- Backup Auto-Attendant and correct menu number
- Account Code settings for each user group

CSIS exposes a list of account code names and numbers within Call Manager clients to facilitate the account selection process for the user.

3.1.6.4 SoftSwitch

SoftSwitch is used to host virtual users who are not assigned a physical telephone port on any ShoreGear voice switch. The SoftSwitch hosts all voice mail, Auto-Attendant, and Workgroup extensions as well as route points. There is a major impact to the system when the SoftSwitch is down or having problems. Loss of connectivity to the SoftSwitch makes the voice mail, Auto-Attendant, Workgroups, and route points supported by the SoftSwitch unavailable.

The SoftSwitch receives and transmits information using the same communication paths and protocols as the "hard" switches in the system.

A SoftSwitch is automatically created for every server added to the ShoreTel system. By default, the name of the SoftSwitch is the same as the name of the ShoreWare server hosting the switch, as specified on the Application Server page in ShoreWare Director. For more information on editing the SoftSwitch parameters, see the *ShoreTel 7 Administration Guide*.

3.2 Maintenance

3.2.1 Server Software Upgrades

An installation of the server software refers to the first time the software is installed on a server. This takes place only once and can be done with any version of ShoreWare software.

Server software upgrades take place any time new ShoreTel software is loaded. The Setup program detects the installed software and automatically takes care of converting any system files or databases. In general, you can upgrade any two previous major versions of the ShoreTel software to the current major version.

Upgrading from one minor version to another automatically converts any system files or databases. Minor upgrades typically add incremental features to the software or correct product defects found in previous releases.

3.2.2 Recommended Files to Backup

It is recommended that you save the contents of the ***Shoreline Data*** directory and all subdirectories to a safe location before performing any significant offline maintenance, including system upgrades or installing security patches or service packs. Typically, backing up the ***Shoreline Data*** directory copies every dynamic file necessary to recover a ShoreTel system.

You may not want to backup the ***Shoreline Data\logs*** directory since this information is not necessary to recover the system and the files are often quite large.

At a minimum, it is recommended that you back up the ***Shoreline Data\Database\ ShoreWare.mdb*** file after making database changes. This allows you to recover the entire ShoreTel system with the exception of saved voice mail, personal names and greetings, and menu and workgroup prompts.

3.2.2.1 Workgroup and Auto-Attendant Prompts

It is recommended that you store a copy of any Workgroup and Auto-Attendant prompts in a safe location, with the .wav files identified by their use. These files are located in the ***Shoreline Data\Prompts*** directory in the format *user-YYYYMMDD-HHMMSS*.wav where *user* is the name of the ShoreTel extension that was used to record the prompts. *YYYYMMDD-HHMMSS* is the time the file was saved. ShoreTel recommends renaming the file to reflects its use, for example, MainAAOnHoursprompt.wav.

3.2.2.2 Voice Mail and Auto-Attendant System Files and Messages

Files located in the VMS directory include voice mail "pointers," user names, greetings, and current voice mail messages. You may save these files as a backup, but be careful when using them to restore a system. Keep in mind that these files reflect the particular time a backup was made. The voice mail system is a dynamic, transaction-oriented system. Any transactions that occurred after the last backup will be lost.

The ***Shoreline Data\VMS*** directory and subdirectories also include all voice mail greetings for each user.

3.3 Diagnostic and Troubleshooting Information

The ShoreTel system provides information about the operational status of the servers and services, as well as diagnostic and troubleshooting tools to resolve an event or error that might occur while the system is running or during installation.

3.3.1 Installer Logging

Some logging information can be gathered by the installer technology native to the operating system. However, ShoreTel has added proprietary code that provides more detail in the log files to assist you in troubleshooting software installation. This proprietary code adds information about calls to the installer and return values from all custom action functions invoked by the installer.

Log files are generated in the user profile temp directory and start with *msi* and end with *.log*. We recommend sorting the directory if there are many log files or if there is any doubt as to which log file to look at.

3.3.1.1 Configuring Installer Logging

To configure Installer Logging, the following procedure must be performed on the server that will be running the ShoreTel software ***before*** the software is installed on the system.

Step 1 Click on the **Start** bar and select **Run**.

Step 2 Type "**regedit**" to access the Registry Editor window.

Step 3 Navigate to the following path:

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]

Step 4 Right-click in the blank pane at the right of the window and select **New > String Value**.

Step 5 Name the file "**Logging**".

Step 6 Right-click on the file and select **Modify**.

Step 7 In the **Value data** field, type "**voicewarmup!**" as shown below.

Step 8 Click **OK**.

There are no obvious signs that installer logging has been enabled. However, after you have enabled the feature (and performed a software installation), you can check the temp directory for log text files at the following location.

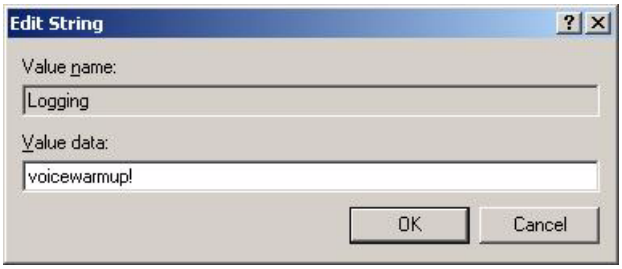

Figure 3-4 Enter the Value Data Information

C:\Documents and Settings\username\Local Settings\Temp

Details

- After Installing Logging has been enabled, you may see installation logs appear in the temp directory for other non-ShoreTel software installations.
- You may have to change the setting for the file view features in Windows Explorer so that hidden files, directories, and file extensions are visible.

3.3.2 Using Quick Look

Quick Look, which is available from ShoreWare Director, gives the system administrator an overview of the ***ShoreTel 8*** system's health. It includes information about each site and the corresponding switches, ports, servers, and service. This is the first place you should look to determine the status of the system.

For details about Quick Look, please see the "Maintenance" chapter of the *ShoreTel 7 Administration Guide*.

3.3.3 Using the Event Log

The ShoreTel system uses the Windows Event Log, viewed using the Event Viewer, to report information and errors that are of interest to system administrators. You can use the event logs in conjunction with Quick Look to determine the overall health of the system. You can also use the event log to gather information about an event that is no longer a problem. For example, the event log may provide information about an overnight T1 outage that was corrected is no longer evident.

Each system task reports when it starts and stops. These messages can be helpful in determining whether the system has started correctly. Events, such as switches losing connection to the server or rebooting, are also reported. See Appendix A, starting on page 143 for a list of all ShoreTel event codes.

3.3.4 Using the System Logs

The ShoreTel system stores a number of engineering-level log files that record transaction information about every event in the ShoreTel system. The logs are used to help ShoreTel with debugging problems that may arise during system operation. In most cases, these logs are difficult to interpret and will require the assistance of ShoreTel Customer Support to understand.

Either of two utilities can be used to automate the collection of server logs, Windows (OS) logs, and ShoreWare databases. The utilities include a graphical application (i.e. GUI) and a command line application. Both applications have the same functional capabilities and offer two different ways for accomplishing the same tasks.

3.3.4.1 Graphical Application

The graphical application can be executed from MS Windows or from a command window. The following program launches the Graphical version of the Server Log Collection Utility:

<*ShoreWare install directory*>\slogWin.exe

where <*ShoreWare install directory*> is the location of the ShoreWare server files. The default installation location of ShoreWare server files is

C:\Program Files\Shoreline Communications\ShoreWare Server.

Panels provide ***Next*** and ***Back*** buttons for navigating through the process. You can terminate the program at any time by pressing the ***Cancel*** button

Banner Panel

The Server Log Utility displays the Banner panel, shown in Figure 3-5, when you execute the Graphical Application. Press the ***Next*** button to proceed to the Date Selection panel.

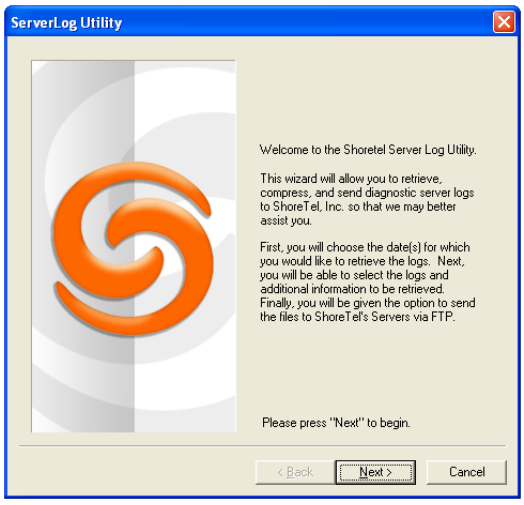
ServerLog Utility
Welcome to the Shoretel Server Log Utility.
This wizard will allow you to retrieve, compress, and send diagnostic server logs to ShoreTel, Inc. so that we may better assist you.
First, you will choose the date(s) for which you would like to retrieve the logs. Next, you will be able to select the logs and additional information to be retrieved. Finally, you will be given the option to send the files to ShoreTel's Servers via FTP.
Please press "Next" to begin.
< Back
Next >
Cancel

Figure 3-5 Graphical Server Log Utility – Banner panel

Date Selection panel

The Date Selection panel, shown in Figure 3-6, specifies the dates for which the log files are collected. The program collects files only for a contiguous date set. The default selection is today's date.

- **To select today's date**, press the **Next** button without modifying the panel contents.
- **To select a single date**, click on the desired date with the mouse cursor.
- **To select a date range**, click and hold on the first day in the range, then drag the cursor to the last day in the range. The maximum range is seven days.

Press the *Next* button to proceed to the Log Selection Method panel.

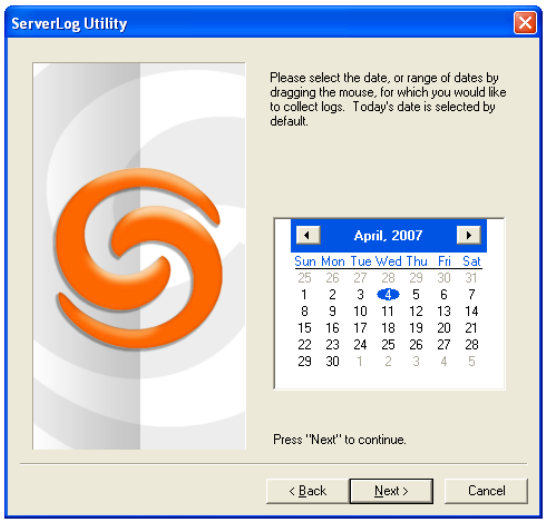
ServerLog Utility
Please select the date, or range of dates by dragging the mouse, for which you would like to collect logs. Today's date is selected by default.
April, 2007
Sun Mon Tue Wed Thu Fri Sat
25 26 27 28 29 30 31
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 1 2 3 4 5
Press "Next" to continue.
< Back
Next >
Cancel

Figure 3-6 Graphical Server Log Utility – Date Selection panel

Log Selection Method panel

The Log Selection Method panel, shown in Figure 3-7, specifies the log file selection method and the destination directory.

ServerLog Utility
Please choose the log selection method you prefer.
Default All ShoreTel logs and databases, and all system logs.
Custom Manually choose which logs to collect.
Destionation Directory
C:\Shoreline Data\Logs
Browse...
Press "Next" to continue.
< Back
Next >
Cancel

Figure 3-7 Graphical Server Log Utility – Log Selection Method panel

Log Selection Method

- **To select all log files for inclusion in the archive**, select the ***Default*** radio button.

  Press the ***Next*** button while ***Default*** is selected to begin archiving all available log files.

- **To manually select the desired log files for inclusion in the archive**, select the ***Custom*** radio button.

  Press the ***Next*** button while ***Custom*** is selected, to open the ***Log Selection*** panel. This panel prompts you to select the log files for inclusion in the archive.

Destination Directory Selection

The destination directory is listed above the ***Browse*** button.

- **To select the Destination Directory**, press the ***Browse*** button

  The program opens a **Browse for Folder** panel for selecting the Destination directory.

Log Selection panel

The Log Selection panel, shown in Figure 3-8, specifies the log files that the program archives. The utility does not display this panel if you select ***Default*** in the Log Selection Method panel.

The four options at the top of the panel select multiple log files. When you select one of these options, all log files included by that selection are selected and cannot be edited. Select *ALL* to include all files in the archives.

All available log files are listed below the first four options at the top of the panel. You can select one file, all files, or any combination of files. Available log files are shown in Figure 3-8 below.

Press the ***Next*** button to begin saving log files.

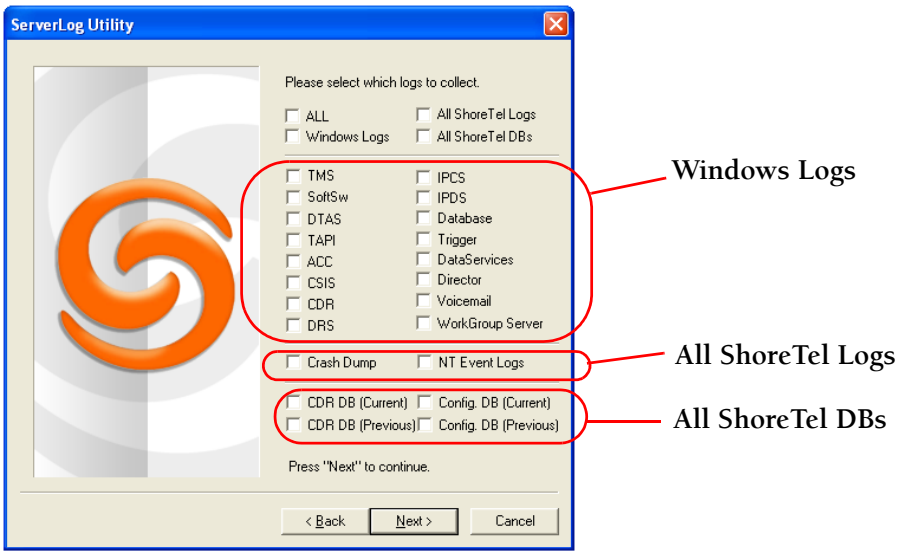

Figure 3-8 Graphical Server Log Utility – Log Selection panel

Archiving Panel

The utility displays the Archiving panel, shown in Figure 3-9, while the program[1] saves the selected files. The ***Next*** and ***Back*** buttons are disabled while the program is saving the files. The ***Cancel*** button remains available.

Press the ***Next*** button after the Save process is completed to display the FTP Upload panel.

1. Parts of the 7-Zip program, licensed under GNU LGPL, are used to compress and create archive files. For more information, see the following website: www.7-zip.org

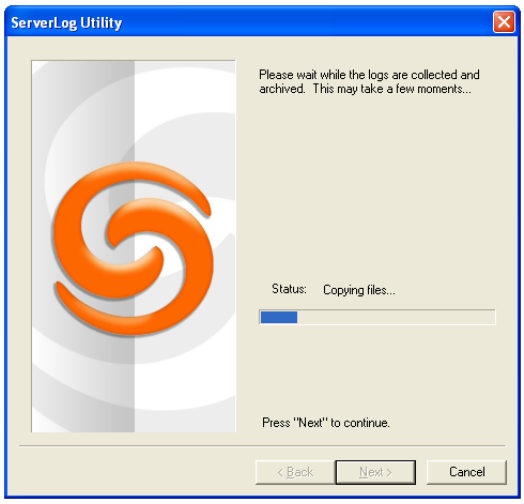
ServerLog Utility
Please wait while the logs are collected and archived. This may take a few moments...
Status: Copying files...
Press "Next" to continue.
< Back
Next >
Cancel

Figure 3-9 Graphical Server Log Utility – Archiving panel

FTP Upload panel

After archiving the files, the program presents an option to upload the archive file to a remote FTP server, as shown in Figure 3-10. Enter valid settings for all FTP parameters, then press the ***Upload*** button.

Press the ***Next*** button to proceed to the Completion panel.

Figure 3-10 Graphical Server Log Utility – FTP Upload panel

Completion Panel

The Completion panel, shown in Figure 3-11, indicates that the log files were successfully archived to the specified directory.

Press the ***Finish*** button to close the utility.

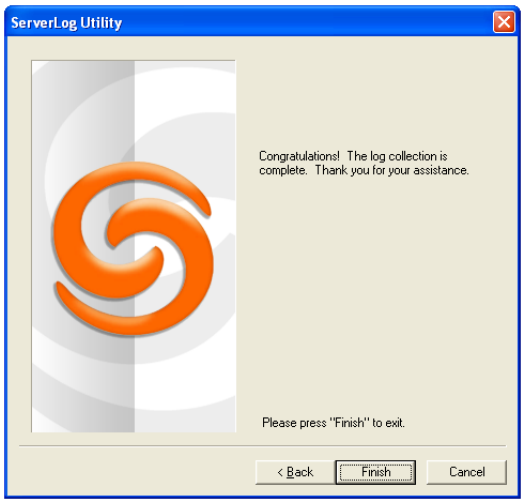

Figure 3-11 Graphical Server Log Utility – Completion panel

3.3.4.2 Command Line Application

The Command Line version of the Server Log Collection Utility provides the identical functionality as the Graphical application from the windows command prompt. The following program launches the Command Line version of the Server Log Collection Utility:

<*ShoreWare install directory*>\ServerLog.exe

<*Shoreware install directory*> is the location of the ShoreWare server files. The default installation location of ShoreWare server files is ***C:\Program Files\Shoreline Communications\ShoreWare Server***.

The following is a complete set of available command line parameters:

ServerLog.exe [-d1 <date1>] [-d2 <date2>] [-CDRDB] [-CONDB] [-CRASH] [-NTEL] [-TRIG] [-DB] [-DIR] [-DS] [-WGS] [-VM] [-IPDS] [-IPCS] [-DRS] [-CSIS] [-ACC] [-CDR] [-TAPI] [-DTAS] [-SS] [-TMS] [-ALLCONDB] [-ALLCDRDB] [-ALLWIN] [-ALLDBS] [-ALLLOGS] [-ALL] [-d <destDir>] [-f] [-v] [-h] [<path> <user> <pass>]

WHERE:

-d <destDir>	Set Destination Directory. **This is a mandatory parameter.**
-d1 <date1>	Set Start Date. date1 = mmddyy.
-d2 <date2>	Set End Date. date2 = mmddyy.

If -d1 is not specified, <date1> and <date2> are both set to the current date.

If -d1 is specified, -d2 becomes a mandatory parameter where <date2> must be greater than or equal to <date1> and less than (<date1> + 7 days).

-CDRDB	Retrieve current CDR Database Log
-CONDB	Retrieve current Configuration Database Log
-CRASH	Retrieve Crash Dump Logs
-NTEL	Retrieve NT Event Logs
-TRIG	Retrieve Trigger Logs
-DB	Retrieve Database Logs
-DIR	Retrieve Director Logs
-DS	Retrieve DataServices Logs
-WGS	Retrieve Workgroup Server Logs
-VM	Retrieve Voicemail Logs
-IPDS	Retrieve IPDS Logs

-IPCS	Retrieve IPCS Logs
-DRS	Retrieve DRS Logs
-CSIS	Retrieve CSIS Logs
-ACC	Retrieve ACC Logs
-CDR	Retrieve CDR Logs
-TAPI	Retrieve TAPI Logs
-DTAS	Retrieve DTAS Logs
-SS	Retrieve SoftSwitch Logs
-TMS	Retrieve TMS Logs
-ALLCONDB	Retrieve All Configuration Database Logs
-ALLCDRDB	Retrieve All CDR Database Logs
-ALLWIN	Retrieve All Current Windows Logs (ShoreTel, NT Event, Crash Dump)
-ALLDBS	Retrieve All ShoreTel Database Logs (CDR, Config)
-ALLLOGS	Retrieve All Current ShoreTel Logs
-ALL	Retrieve All retrievable logs and databases
-f	Upload the archive to the specified FTP server
<path> <user> <pass>	Specifies the FTP destination location when uploading the archive to an FTP server
-v	Display version number of command line program, then exit
-h	Display name and description of command line parameters, then exit

Example: The following command line copies Voice Mail logs generated between 2 March 2007 and 6 March 2007 to C:\LogsDir directory:

ServerLog.exe -d1 030207 –d2 030607 –VM –d “c:\LogsDir”

Example: The following command line copies all Voice Mail logs generated today:

ServerLog.exe –d “c:\LogsDir”

Example: The following command line generates an error message because only one date is specified:

ServerLog.exe -d1 030207 –VM –d “c:\LogsDir”

3.3.5 Using the Trunk Test Tool

The Trunk Test tool is a TAPI application that monitors real-time activity on a trunk. You can find the tool in the ShoreTel program folder. Figure 3-12 shows the Trunk Test tool interface.

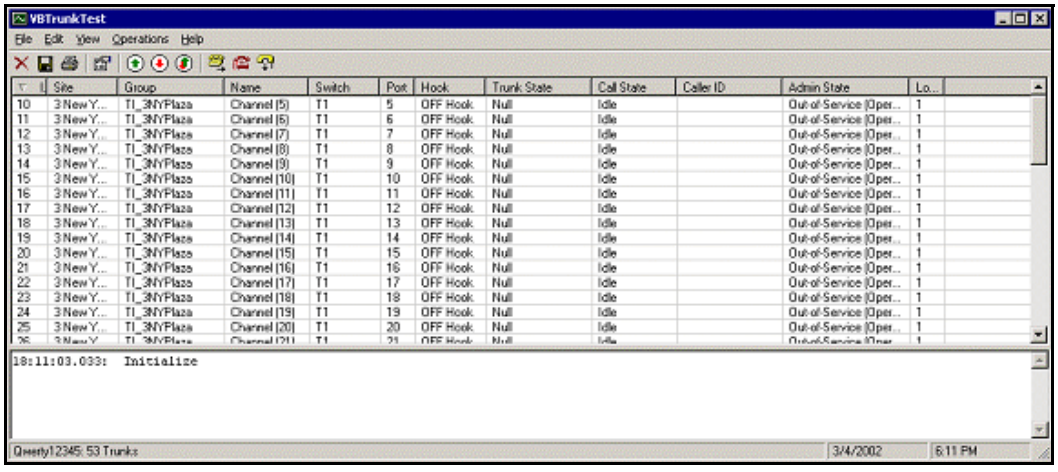
VBTrunkTest
File Edit View Operations Help
Site Group Name Switch Port Hook Trunk State Call State Caller ID Admin State Lo...
18:11:03.033: Initialize
Qwerty12345: 53 Trunks
3/4/2002
6:11 PM

Figure 3-12 Trunk Test Tool

The tool is divided into two sections (see Figure 3-12). The top section lists all the trunks in the system and their current status. The bottom section gives real-time monitoring information about the currently highlighted trunk.

The ***File*** menu allows you to save log information to disk or print it.

The ***Edit*** menu allows you to copy and paste data from the Trunk Test window.

The ***View*** menu allows you to turn on and off the status and toolbars, and open the Trunk Helper Settings dialog box.

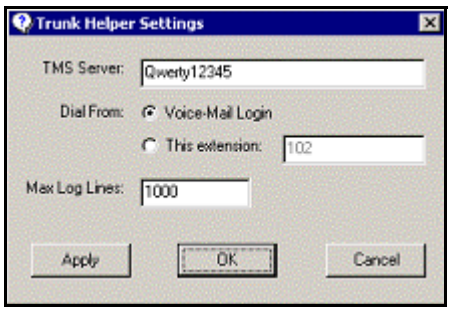

Figure 3-13 Trunk Helper Settings Dialog Box

The ***Trunk Helper Settings*** dialog box allows you to set the server you want to monitor, select an extension to dial out with, and set the number of lines of data to collect for each trunk.

If this tool remains running on the server with an excessive number of lines selected, the server may have performance problems.

The ***Operations*** menu allows you to make or drop calls, view the properties of selected trunks, place trunks in service, and remove them from service. You can also access this menu by right-clicking a selected trunk.

The ***Help*** menu displays the version number of the Trunk Test tool.

3.3.6 Using TapiTest

TapiTest is a command-line TAPI application that lists all the phone and line devices supported by TMS. You can use this as an alternative method to check that a given IP phone is configured and connected, or to get a view of TAPI lines and extensions on the system. TapiTest is included on the ShoreWare DVD.

Use `TapiTest > TapiTest.txt` to dump the output to a text file.

3.3.7 Using the cfg Utility

The **cfg** utility is a command-line tool that provides detailed information about the voice mail application.

Cfg.exe can be found in the ***\shoreline communications\shoreware server*** directory.

To start cfg:

Step 1 Open a DOS window pointing to the ***\shoreline communications\shoreware server*** directory.

Figure 3-14 TapiTest Output

Step 2 Enter `cfg` and press Enter.
When you see the prompt `/*Local*//->`, cfg is ready.

All commands are entered at the above prompt. Results are displayed in the DOS window or in the voice mail logs.

WARNING Some **cfg** utility commands may damage the system if used incorrectly. Make sure you understand the commands before you use them.

Table 3-1 summarizes the commands available through the **cfg** utility. Variables are shown in italics.

Command	Parameters	Description	Comments
call *p*	*p* = phone number	Make a call from the voice mail application and play a prompt.	
closem		Close the open voice mail box.	
dmask *0x*	*0x* = mask hex	Set voice mail debug mask in hex.	To see a list of available flags, enter without a parameter.
exit		Leave cfg.	

Table 3-1 cfg Commands

Command	Parameters	Description	Comments
laam *t*	t = (1 = DID, 2 = DNIS, 3 = Trunk)	List Auto-Attendant menu mapping.	Displays mapping of trunks to Auto-Attendant menus.
lall *f*	f = 1 for more details	List all mail boxes in the system.	Enter without "1" for a summary of system mail boxes and with "1" for more detail.
lamp *m f*	*m* = mail box *f* = (1 = on, 2 = off)	Turns the message waiting light on/off for a specified mail box.	
list pb b	b = (0 = last name, 1 = first name)	Dump dial by names directory to the voice mail log.	
lmbox *f*	f = 1 for more details	List mail box information.	Enter without "1" for a summary of system mail box information, including messages IDs.
lms		List mail box schedule.	
lmsg *m*	*m* = message ID	List details about a specific message.	Message IDs can be found by using lnbox.
loadc		Load all voice mail configuration from the database.	
loadm		Load all mail box configuration from the database.	Requires that a mail box be open when you issue the command.
lserv		List information about all servers.	
lsys		List all voice mail system parameters.	
lsmtp		List status of distributed voice mail.	
ltapi		List status of TAPI lines opened by voice mail.	
msinfo		Dump voice mail internal table to the voice mail log.	
openm #	# = mail box	Open specified mail box.	
psinfo		Dump port server information to the voice mail log.	
purge		Remove message in the deleted queue.	Requires that a mail box be open when you issue the command.
sh *str*	*str* = string	Search help for a string.	Searches only from the beginning.
starth		Remove old deleted messages.	
symwi		Run message waiting indication synchronization.	Sends current MWI status to all phones in the system.
ver		List cfg version.	
?		List help commands.	

Table 3-1 cfg Commands

3.3.8 Using Dr. Watson

Dr. Watson is an application debugging program included with the Microsoft Windows operating system. ShoreTel recommends using the Dr. Watson application if you are running on Windows 2003 Server.

Enabling Dr. Watson

Step 1 Open the **Control Panel** and then double-click **System**.

Step 2 Click on the **Advanced** tab.

Step 3 Click on the **Error Reporting** button. Disable it, or if you choose to enable it, leave it enabled just for the **Windows operating system** and leave the **Programs** checkbox clear.

This must be done whenever a new machine is built or ghosted.

Figure 3-15 Error Reporting window

Step 4 Install Dr. Watson from the command line by typing "drwtsn32 -i"

Step 5 Run "drwtsn32" to configure it. A window similar to the one shown below appears:

Step 6 Under **Crash Dump Type**, select the **Mini** radio button.

Step 7 Select the **Visual notification** checkbox. This will ensure that you are aware when a dump has occurred.

Step 8 Select the **Create Crash Dump File** checkbox.

Step 9 Optionally, in case the dump file might be overwritten, it may be helpful to enable the following options by selecting the associated checkboxes:

- Dump Symbol Table
- Dump All Thread Contexts
- Append to Existing Log File

Step 10 Click **OK** to store your changes.

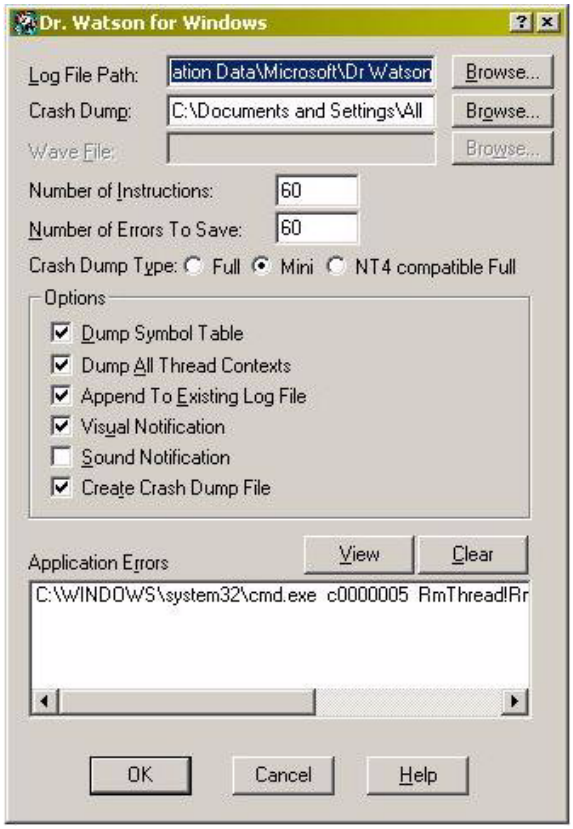

Figure 3-16 Configuring Dr. Watson

To collect Dr. Watson dumps:

- Dumps for a logged in user appear under:
  C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson
- Dumps for services appear under:
  %systemroot%\PCHEALTH\ERRORREP\UserDumps

3.4 Reference

3.4.1 Services (Processes)

The ***ShoreTel 8*** ShoreWare server is made up of multiple processes working together to provide applications that include voice mail, ShoreWare Director, and Workgroups.

Each process runs as a Windows Service, starting automatically when the server starts.

The table below describes each service and its underlying process. All services run on the Headquarters Server. Services that run on distributed servers are marked in the ***Dist. Server*** column.

3.4.2 ShoreWare Server File System

The following list identifies the directories where the ShoreWare server installs its files.

Service Name	Service ID	Process	Description	Dist. Server
ShoreWare Call Accounting	ShoreTel-CDR	TMSCDR.exe	Records call information (call accounting information, call queuing data, and media stream data) and writes it to the CDR database.	
ShoreWare CSIS Server	ShoreTel-CSISSVC	CSISSvc.exe	Provides ShoreWare clients with an interface to the ShoreWare server. Manages voice mail notifications to voice mail clients, and is responsible for managing changes made to the database by the clients.	X
ShoreWare Director Utilities	ShoreTel-DirectorUtil	KadotaUtil.exe	Provides management capabilities for ShoreWare Director. Enables Quick Look to control services and browse the Event Log.	X
ShoreWare Event Watch Server	ShoreTel-EventWatch	EventWatch.exe	Monitors the NT Event Log and delivers email notifications of selected events.	X
ShoreWare IP Phone Configuration Server	ShoreTel-IPCS	IPCSService.exe	Manages the IP phone configuration process, including configuration files and the database updates.	
ShoreWare IP Phone Display Server	ShoreTel-IPDS	IPDS.exe	Controls any actions by the IP phone display not controlled by the device's firmware or switches.	
ShoreWare Notification Server	ShoreTel-Notify	TriggerServer.exe	Notifies server applications of changes to the ShoreWare configuration.	X
ShoreWare Port Mapper	ShoreTel-Portmap	PortMap.exe	Initiates RPC communication connections between the Telephony Management Server (TMS) and ShoreGear switches.	X
ShoreWare Software Telephony Switch	ShoreTel-SoftSwitch	VTSMain.exe VTSService.exe	The SoftSwitch hosts call endpoints for voice mail, Workgroup, route points, and other IVR extensions. Virtual users are hosted on the Headquarters SoftSwitch.	X
ShoreWare Distributed Routing Service	ShoreTel-DRS	DRS.exe	When active, this service provides location information for routing inter-site calls and additional routing information for trunk group selection.	X
ShoreWare Telephony Management Service (TMS)	ShoreTel-TMS	Tms.exe	The telephony platform for ShoreWare applications, ShoreWare services, and third-party TAPI applications.	X
ShoreWare Voice Mail Message Server	ShoreTel-MailServ	MailServ.exe	Service component of the ShoreWare voice mail system.	X
ShoreWare Voice Mail Application	ShoreTel-Vmail	VMail.exe	Service component of the ShoreWare voice mail system.	X
ShoreWare Voice Mail Port Manager	ShoreTel-PortMgr	PortMgr.exe	Service component of the ShoreWare voice mail system.	X
ShoreWare Distributed Telephony Application Server	ShoreTel-DTASSvc	DTAS.exe	Provides distributed telephony to application.	X

Table 3-2 Service Descriptions

Service Name	Service ID	Process	Description	Dist. Server
ShoreWare Workgroup Server	ShoreTel-WGSvc	WorkgroupServer.exe	This service manages workgroups, queues, and call distribution to agents.	
ShoreWare Database Management Service	ShoreTel-Zin	ZinManager.exe	Manages and updates the ShoreWare database via Microsoft's DCOM protocol.	
ShoreWare Account Code Collection Server	ShoreTel-ACC	ACC.exe	Provides account code services for collection and validation.	

Table 3-2 Service Descriptions

The server installs files with default access permissions. (System administrators may want to ensure a more secure environment.)

The Windows System user and the IPBX user created by the ShoreTel installer require full access to all the ShoreWare directories. All other users can be granted access on an as-needed basis.

To ensure the security of sensitive and/or personal information, confine access to the VMS and Database directories strictly to administrator, system, and IPBX users.

- **ShoreWare Server:** Contains all ShoreWare server system files and dlls. This directory is located on the drive where program files are stored: <drive>\program files\Shoreline Communications\ShoreWare Server.
- **ShoreWare Director:** Contains all ShoreWare Director Web site files. This directory is located on the drive where program files are stored: **<*drive*>**\program files\Shoreline Communications\ShoreWare Director.
- **Shoreline Data:** Contains all the dynamic information the server uses to run the system. This directory and all sub-directories may be saved as part of a backup and used for full system recovery. <drive>\Shoreline Data
- **Call Records 2**: Contains all call record files and databases

  The root directory contains Microsoft Access database files used by ShoreWare prior to Version 7.0 for managing call detail records and includes,CDR.mdb, three months of archive files, and one month of legacy text call records.

  Data subdirectory contains MySQL database files used by ShoreWare Version 7.0 for managing call detail records and text files that can be accessed by some legacy CDR storage devices. The CDR database is used by the ShoreWare 7 for compiling standard reports.

  The MySQL database is ODBC compliant. Parameter settings required to access CDR records in the MySQL database include

  — DRIVER={MySQL ODBC 3.51 Driver}
  — SERVER = localhost (or the server where you have MySQL installed)
  — DATABASE = shorewarecdr
  — USER =st_cdrreport
  — password =passwordcdrreport
- **Database:** Contains the configuration database ShoreWare.mdb. This file stores all system configuration information and should be backed up regularly.<*drive*>\Shoreline Data\Database

  The ShoreWare database is stored in a Microsoft Jet 4 database file. The file is designed for application-level management by ShoreWare Director and other

ShoreWare applications. While you can use Microsoft Access to view and troubleshoot consistency problems, do not attempt to modify the database with any other applications.

- **Logs:** Contains all ShoreTel debugging logs.
  <*drive*>\Shoreline Data\Logs
- **Prompts:** Contains copies of the menu prompts.
  <*drive*>\Shoreline Data\Prompts
- **Scripts:** Contains scripts used by the Workgroup Server.
  <*drive*>\Shoreline Data\Scripts
- **SoftSwitch:** Contains files needed to run the SoftSwitch. <*drive*>\Shoreline Data\SoftSwitch
- **Templates:** Contains configuration files needed for IP phones.
  <*drive*>\Shoreline Data\Templates
- **VMS:** Contains all the files and configuration information used by the voice mail system. The files in this directory and its sub-directories are very dynamic and should never be opened. Opening any of the configuration files may cause the voice mail system to become corrupted in part or completely, and can cause loss of voice mail messages.
  <*drive*>\Shoreline Data\VMS
- **MESSAGE:** Contains all voice mail messages as .wav files, along with an .enl pointer file for each message.
  <*drive*>\Shoreline Data\VMS\MESSAGE
- **NetTempIn:** Used by distributed voice mail servers.
  <*local drive*>\Shoreline Data\VMS\NetTempIn
- **Servers:** <*drive*>\Shoreline Data\VMS\Servers
- **ShoreTel:** Contains a subdirectory folder for each voice mail box configured on the system. Each user, menu, and distribution list has a mail box. There are also system mail boxes for voice mail access and forwarding. Each of the sub-directories contain the names and greetings for that mail box, as well as configuration and pointer files.
  <*drive*>\Shoreline Data\VMS\SHORETEL
- **Inetpub\ftproot:** This is the default FTP directory installed by IIS.
  <*drive*>\Inetpub\ftproot
- **ts12:** Contains the boot files and system software for the ShoreGear 12 and ShoreGear Teleworker.
  <*drive*>\Inetpub\ftproot\ts12
- **ts24:** Contains the boot files and system software for the ShoreGear 24.
  <*drive*>\Inetpub\ftproot\ts24
- **tsa:** Contains the boot files and system software for all ShoreGear 40/8, 60/12, 120/24, T1 switches.
  <*drive*>\Inetpub\ftproot\tsa
- **tst1:** Contains the boot files and system software for earlier versions (pre-2004) of the ShoreGear T1 and ShoreGear E1. <*drive*>\Inetpub\ftproot\tst1

3.4.3 Registry

The ShoreTel software utilizes the Windows registry to store various parameters used by the ShoreTel system. These registry keys can be found in the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks

3.4.4 ShoreTel Release Numbering Scheme

In the ShoreTel release number schema, the first number is the major build, second is the minor build, the third is the number of the build, and the fourth number is always 0.

The following guidelines are used in the ShoreTel version numbering schema:

- Major = release; minor = update within release; build = build number of the minor/major combo; fourth number = 0
- DVD or Package major.minor.build.0
  - Example 8.3.1601.0
- Server major.minor.build.0
  - Example 8.3.1601.0
- Remote Server major.minor.build.0
  - Example 8.3.1602.0
- Client major.minor.build.0
  - Example 8.3.1603.0
- Switch major.minor.build.0
  - Example 8.3.1604.0

Patches are software fixes that update a specific version of software and cannot be applied to previous major or minor versions.

CHAPTER 4

ShoreGear Switches

4.1 Overview

ShoreTel ShoreGear voice switches provide physical connectivity for the PSTN and analog phones, and logical connectivity for IP endpoints on a reliable, highly scalable platform for the ShoreTel call control software. The call control software runs on top of VxWorks, a real-time embedded operating system designed specifically for mission-critical applications.

The voice switches have flash memory that allows permanent storage of the call control software and configuration information. The voice switches have no moving parts (that is, no hard drive) other than a highly reliable fan. The switches include the necessary DSP technology to enable toll-quality voice with features like echo cancellation, voice compression, and silence suppression.

TMS propagates configuration data from the database to each switch upon reboot of either TMS or the switch. The data sent is a subset of configuration data specific to that switch. TMS also maintains this data by propagating changes to the database to those switches affected by the change. The TMS/Switch configuration interface uses the same Network Call Control protocol that is used for other TMS/switch communication. The NCC protocol is based on Sun RPC. You can obtain the configuration data that TMS sends to any specific switch with a CLI command. For more information, see Section 4.3.2.1 on page 59.

Switches share their switch-specific configuration with other switches in the system using the UDP-based Location Service Protocol (LSP). Switches keep current with other switches by propagating their changes and receiving them from other switches. For information about viewing switch-to-switch communications, see Section 4.3.2.1 on page 59.

The ShoreGear voice switches communicate call control information on a peer-to-peer basis. When Distributed Routing Service (DRS) is enabled, switches exchange LSP messages only with other switches at the same site. DRS communicates directly with the database to keep the database configuration current. TMS tells each switch how to find DRS as part of the configuration process described earlier. When DRS is enabled, switches generally give DRS an opportunity to resolve numbers, so that its more complete view of the system can be leveraged to find the best contact. If the switch knows where an intra-site extension is, it does not involve DRS.

For analog phones, the switch detects whether the phone is on or off hook, collects digits from the phone, and—based on digits collected—determines when a call should be established. If necessary, the switch communicates with other switches (in some cases this may not be necessary, such as when call is to an endpoint directly on the switch) to establish a call between the appropriate endpoints.

The switch acts as a media gateway for the PSTN and analog phones by encoding the analog voice and transmitting it to the other endpoint over the IP network using RTP. The switch also uses NCC to send events to TMS about digit collection, caller ID, call establishment, and so forth. TMS makes this information available to the server applications. These applications are not necessary for many calls (such as those between two phones or a trunk and a phone, which can be established with only the switches

controlling the phones and trunks), but they can enhance the user experience. For example, Personal Call Manager can provide information about the call to the user's desktop.

Once the call is established, TMS monitors the call and logs call information on the Call Detail Report (CDR) database.

4.2 Maintenance

4.2.1 ShoreGear Firmware Upgrades

Each ShoreGear switch is shipped from the factory with the version of firmware that ShoreTel used to test the system.

When you install a switch, ShoreTel's TMS service is set up to detect the switch's firmware version and automatically upgrade your hardware to the latest version. This happens once while the switch still retains the factory-default settings. (You can use the ShoreWare Director Quick Look page to monitor the progress of the upgrade.)

ShoreTel also makes firmware upgrades available via system upgrades and patches.

4.2.1.1 Using Quick Look to Perform Upgrades

You can use the Shoreware Director Quick Look page to identify switches that require upgrades. When a switch update is required, QuickLook reports ***Firmware Update Available*** or ***Firmware Version Mismatch***.

- **Firmware Update Available** indicates that a patch is available and an upgrade is required to load the patch. When a switch is in this state, it is fully functional and in communication with TMS and the other switches in the system.
- **Firmware Version Mismatch** indicates that you must upgrade the switch before it can communicate with the TMS server. When a switch has mismatched firmware, it can still communicate with other switches of the same version and manage calls, but cannot support server and client applications.

To upgrade the switch:

Step 1 In ShoreWare Director, open the ***Maintenance > Quick Look*** page, and select the Site where the switch is located. Choose Reboot from the Command drop-down list in the switch row.

Upon restart, the switch is automatically upgraded. You can monitor the progress of the upgrade on the Quick Look page.

4.2.1.2 Performing a Manual Upgrade

To manually upgrade the switch's firmware:

Step 1 From the server command line, enter the *burnflash* command in this format:

```
C:\Program Files\Shoreline Communications\ShoreWare
Server>burnflash -s <switch IP Address>
```

4.2.2 ShoreGear Switch Boot Options

When a ShoreGear voice switch boots, it requires an IP address to connect to the network and an application program. ShoreGear voice switches are set to use a DHCP server for an IP address and to retrieve the application from the switch's flash memory.

If a DHCP request receives no response, the switch tries a BootP request as a backup. ShoreTel recommends using static IP parameters configured via the serial port, as this is much more reliable. If DHCP is to be used, ShoreTel strongly recommends using DHCP reservations for each switch so that the DHCP lease will not be lost.

If a DHCP server is not available, you can set the IP address manually from the switch's maintenance port. The ShoreGear-12 and ShoreGear-Teleworker voice switches can be set to use a static IP configuration via a Telnet session after they have received an IP address via DHCP or BootP.

The standard method for booting a ShoreGear voice switch is to boot from the switch's flash memory. When a ShoreGear switch is first powered on, it reads the boot parameters stored on the boot ROM, which instructs the switch to load software from flash memory. When the software starts, it loads its configuration, which is also stored in flash memory.

Booting from FTP is available for instances when you cannot boot the switch from flash memory. When you boot a switch from FTP, the operating system and software load from the FTP site identified in the boot parameters. The loaded configuration is a configuration received from the TMS server.

If the switch fails to load the application from flash and does not have the IP address of the ShoreWare server, you can set the IP address and boot parameters by connecting to the maintenance port and using the configuration menu. The configuration menu allows you to set the IP address of the switch and enter the ShoreWare server (boot host) IP address.

4.2.2.1 IP Address from DHCP

The switch sends requests for an IP address to the DHCP server ten times at increasing intervals. When the switch receives a response from the DHCP server, the boot process begins. If the switch fails to get an IP address from the DHCP server, it uses the last assigned IP address. The switch continues sending IP address requests to the DHCP server.

If the DHCP server sends a conflicting IP address while the switch is using an address from a previous state, the entire system restarts. Use long lease times to prevent to prevent this. ShoreTel recommends either static IP parameters or DHCP reservations.

If the switch does not receive an IP address from the DHCP server and an address is not available from a previous state, the switch continues polling the DHCP server until it receives an address.

4.2.2.2 Setting the IP Address with VxWorks

If the switch has not been configured with an IP address and fails to boot from flash, it will not be able to download the application and configuration from the FTP server. In this case, you can manually set the IP address and boot parameters from VxWorks accessible from the maintenance port.

Boot parameter changes do not take effect until the switch is rebooted.

This command line interface is not available through Telnet.

To connect to the maintenance port of a ShoreGear voice switch:

Step 1 Connect a serial cable between a personal computer and the ShoreGear switch.

Step 2 Use a terminal emulation program such as Tera Term Pro freeware to open a connection to the switch.

Step 3 Apply these values to the terminal settings:

- Speed: 19.2 Kbs
- Data bit: 8 bits
- Stop bit: 1
- Parity: No parity
- Flow Control: None

The CLI Main Menu

The CLI main menu automatically appears at system startup. You can also invoke the menu at any time by entering a question mark (?).

The following list describes the commands available in the CLI main menu:

- (1) -- **Show version:** Lists version numbers for firmware and boot ROM in addition to the base version and the CPU board version.
- (2) -- **Show system configuration:** Displays the switch's boot and IP configuration.
- (3) -- **Change system configuration:** Takes you to the system configuration menu where you can set a switch's boot and IP configuration.
- (4) -- **Reboot:** Reboots the switch.
- ? -- **Help:** Enter a ? to print this menu.

To select an option in Shoregear CLI, enter the number associated with the menu item and press ENTER. To change or set a parameter, select the item you wish to change, then type the parameter number and press Enter.

Boot and IP Configuration Options

When you choose Change System Configuration from the CLI main menu, a menu of boot and IP configuration options appears.

- (0) -- **Return to previous menu:**
- (1) -- **Change IP address:**
- (2) -- **Change IP subnet mask:**
- (3) -- **Change gateway IP address:**
- (4) -- **Change server IP address:** This is the IP Address the ShoreWare server with the FTP service for the switch.
- (5) -- **Change boot method:**
- (6) -- **Enable/disable DHCP:**
- (7) -- **Change network speed and duplex mode:**
- ? -- **Help:**

After you have set your IP address and boot options, enter ? to return to the main menu. You must reboot the switch for the new setting to take effect.

4.2.2.3 Accessing ShoreGear CLI on the SoftSwitch

To run ShoreGear CLI diagnostics on the SoftSwitch, you must create a Telnet session. ShoreGear CLI commands are listed in Section 4.3.2 on page 59.

To start a SoftSwitch Telnet session on the server:

Step 1 Create the following DWORD entry in HKey_Local_Machine\Software\Shoreline Teleworks\SoftSwitch:

```
TelnetEnabled
```

Step 2 Set the value to 1.

Step 3 Open a Command Prompt (DOS) window and type:

```
telnet localhost 2323
```

In order to Telnet to the SoftSwitch, the Telnet port must be set to 2323. The standard Telnet port is 23.

Step 4 Press ENTER.

There are no usernames or passwords to enter. This immediately logs you into the SoftSwitch.

Step 5 Press ENTER a second time to get the SoftSwitch prompt.

The prompt is as follows:

```
????
SHELL: ????
SHELL:
```

Step 6 Enter CLI commands as described in Section 4.3.2 on page 59.

Step 7 End the SoftSwitch Telnet session by typing `exit.`

Step 8 Press ENTER.

Step 9 Remove the "Telnet Enabled" DWORD from the registry editor by right-clicking on it and selecting **Delete**.

To start a Telnet session to the SoftSwitch from a different computer, you must specify the IP address of the ShoreWare server and modify the Telnet port to 2323.

All switch commands are available in the SoftSwitch with the exception of the following:

- Any VxWorks-specific commands
- msps

4.2.2.4 Modifying Router Auto-Delete Properties for ICMP Redirects

When WAN links fail, ICMP redirect messages are received by the ShoreGear switches from routers on the network. These ICMP redirect messages notify hosts on the network (i.e. ShoreGear switches) that an alternate route[1] is available and the switch updates its routing table accordingly.

1. The router will most often direct the switch to use the default gateway, and this gateway can often be a device that has no connectivity to the remote site.

If these messages were not deleted from the switch, the routing table could get cluttered with old, useless, or perhaps inaccurate information. Therefore, the default behavior for ShoreGear switches is to automatically delete any ICMP redirect messages after a period of three minutes has expired from the time of receipt.

If desired you can shorten or lengthen this period of time in one-minute increments, or you can disable the automatic deletion of ICMP redirect messages altogether.

To modify the time period for the automatic deletion of ICMP redirect messages, follow the procedure below:

Step 1 Create the following DWORD entry in HKEY_LOCAL_MACHINE\SOFTWARE\Shoreline Teleworks\Telephony Management Server\Settings:

`SwitchDebug - "debug_options timeout_icmp_redirect n."`

Step 2 Set the value of *n* to the desired time period. Note that this must be an integral value and the number represents minutes, not seconds. The value of *n* can be set to zero (0) to disable the autodeletion of ICMP redirect messages.

When this key is defined in the main server, the switches will automatically delete all of their routing table entries after the specified period of time. Note that sampling occurs once per minute, so routes will not disappear exactly 360 seconds later if *n* is set to 6.

Step 3 Reboot the ShoreGear switch for these changes to take effect.

4.2.2.5 Using a Telnet Session to Set IP Address and Boot Parameters

You have the option of setting IP address and boot parameters using the VxWorks `bootChange` command. To access the bootChange command, you must establish a telnet session to the switch. For information on other commands available from VxWorks, see Section 4.3.2 on page 59.

To set IP address and boot parameters via `bootChange`:

Step 1 Start the Telnet process with an *ipbxctl* command entered in this format:

```
C:\Program Files\Shoreline Communications\ShoreWare
Server>ipbxctl -telneton <Switch IP Address>
```

Once the Telnet process is running, open a Telnet session with the switch.

You are prompted for a user name and password.

Step 2 For the user name, enter `anonymous`.

Step 3 For the password, enter `ShoreTel` (case sensitive).

Step 4 At the > prompt, enter `bootChange`.

The boot device parameter appears.

Step 5 Modify parameters by typing values and pressing ENTER [Do not backspace].

When you press ENTER, the next boot parameter appears.

See Table 4-1 for listings of parameters required for flash and FTP booting of ShoreGear switches.

Check the model number on the back of the switch. If model is an IPBX, use the IPBX row. If it is SG, use the SG row.

Step 6 Close the Telnet connection with the following ipbxctl command:

```
C:\Program Files\Shoreline Communications\ShoreWare
Server>ipbxctl -telnetoff <Switch IP Address>
```

Parameter	Description	Flash Boot	FTP Boot		
		24, T1/E1 SG-90/50/ 220T1/220E1	24	T1/E1	SG-90/50/ 220T1/ 220E1
boot device	A network interface or a flash location	flash = 0	fei	fei	emac0
processor number	Always 0	0	0	0	0
host name	Always bootHost	bootHost	bootHost	bootHost	bootHost
file name: IPBX	Path to VxWorks.sys file for IPBX switches	/flash0/vxworks	/ts24/vxworks	/tst1/vxworks	N/A
file name: SG	Path to VxWorks.sys file for SG switches	/flash0/ vxworks	/tsa/ vxworks	/tsa/ vxworks	/tsk/ vxworks
inet – ethernet	<IP address>:<Subnet Mask (hex)>[a]	10.10.0.59: ffff0000	10.10.0.59: ffff0000	10.10.0.102: ffff0000	10.10.0.102: ffff0000
inet – backplane	Not used				
host inet	IP address of the main ShoreWare server[a]	10.10.0.5	10.10.0.5	10.10.0.5	10.10.0.5
gateway inet	IP address of router[a]	10.10.0.254	10.10.0.254	10.10.0.254	10.10.0.254
user	FTP site – User name login (typically set to anonymous)	anonymous	anonymous	anonymous	anonymous
ftp password (pw) (blank = use rsh)	FTP site – Password (typically set to st1)	st1	st1	st1	tsk
flags	See Boot Flags	0x40	0x40	0x40	0x40
target name	Host name of switch that can be set to other values	ShorelineSwitch	ShorelineSwitch	ShorelineSwitch	Shoretelbuild
startup script (IPBX)	Path to bootscrp.txt file for IPBX switches	/flash0/ bootflsh.txt	/ts24/ bootscrp.txt	/tst1/ bootscrp.txt	N/A
startup script (SG)	Path to bootscrp.txt file for SG-24, SG-8, SG-T1	/flash0/ bootflsh.txt	/tsa/ bootscrp.txt	/tsa/ bootscrp.txt	/tsk/ bootscrp.txt
other	Set to network interface	fei	fei	fei	emac

Table 4-1 Parameter Settings for Flash Boot and FTP Boot

a. The IP addresses are examples. These must contain the correct IP addresses for your system.

4.2.2.6 Boot Flags

The boot flags allow you to alter how the switch will boot up. The hexadecimal values of the flags and their actions are listed in Table 4-2.

You can aggregate flags to perform multiple functions by summing the hex values for the commands. For example, the command:

```
0x42040
```

aggregates the flags "0x40 + 0x2000 + 0x40000" and instructs the switch to use DHCP to get boot parameters, disable the ShoreTel shell, and set network speed and duplex mode to 100 Mb HD.

Command	Description
0x0	Network speed and duplex mode auto-negotiate.
0x20	Disable login security.
0x40	Use DHCP to get boot parameters.
0x1040	Use bootp to get boot parameters.
0x2000	Disable ShoreTel shell.
0x10000	Network speed and duplex mode 10 Mb full duplex (fixed).
0x20000	Network speed and duplex mode 10 Mb half duplex (fixed).
0x30000	Network speed and duplex mode 100 Mb full duplex (fixed).
0x40000	Network speed and duplex mode 100 Mb half duplex (fixed).

Table 4-2 Boot Flags

Setting IP Address and Boot Parameters from the VxWorks Boot Monitor

If you are unable to access the ShoreGear CLI, you can access the same configuration options available with the bootChange command from the switch's boot monitor.

WARNING Making the incorrect settings in the boot monitor can cause the switch to malfunction.

To access the boot monitor:

Step 1 Connect a serial cable between a personal computer and the ShoreGear switch.

Step 2 Use a terminal emulation program such as HyperTerminal to open a connection to the switch.

Step 3 Apply these values to the terminal settings:

- Speed: 19.2 kbps
- Data bit: 8 bits
- Stop bit: 1
- Parity: No parity
- Flow Control: None

Step 4 Type `c` at the prompt and press ENTER. You will be guided through the options listed in Table 4-1 on page 55.

4.2.3 ShoreGear Switch Configuration Reset

Each switch has a hidden reset button on the front panel that restores the switch to factory default boot settings and requests a new configuration from TMS. To enable the reset, press the button for 5 seconds. This button reboots the ShoreGear voice switch.

This completely clears all boot parameters and clears the switch's configuration.

4.2.4 ShoreGear Switch Utilities

There are two tools available for diagnosing and updating the ShoreGear voice switches. The *ipbxctl* utility allows one to perform diagnostics and Telnet to the switch. You can use the ***burnflash*** utility to update the switch to the version of firmware compatible with the ShoreWare server software.

The utilities are available in the ShoreWare Server folder:

```
C:\Program Files\Shoreline Communications\ShoreWare Server
```

4.2.4.1 ipbxctl Utility

The following table summarizes the commands available using the ***ipbxctl*** utility:

Command	Description
-telneton <*Switch IP Address*>	Enables Telnet connection on the switch.
-reboot <*Switch IP Address*>	Reboots the switch without using ShoreWare Director.
-flash <*Switch IP Address*>	Sets switch to boot from flash memory (allows you to boot without logging in).
-ftp <*Switch IP Address*>	Sets switch to boot from FTP (allows you to do this without logging in).
-diag <*Switch IP Address* >	Sends switch state information. By default, the system puts this information in the same folder where ipbxctl utility is running. This may be distruptive to normal switch function. Use this command only for diagnostic functions, not for reporting.
-reset	Clears all flash memory. Returns switch to factory defaults. This command is not available from ShoreTel CLI.
-telnetoff <*Switch IP Address* >	Disables Telnet connection on the switch.
-traceroute <*target IP Address* >	Network troubleshooting tool. For additional information about the parameters that can be used with this command, Table 4-6 on page 66 of this chapter.

Table 4-3 ipbxctl Utility Commands

For more information on launching the *ipbxctl* utility, see Section 4.2.2 on page 51.

Password Access

After entering the **ipbxctl** command, the user is prompted to enter a password. After the user enters the correct password, the device permits access to executables that configure or diagnose the switch.

Performing a telnet session on a ShoreGear switch requires password access to ipbxctl before invoking the teleneton command. After entering the correct password, a user can establish of a telnet session during the next minute. At the expiry of this period, existing telnet sessions are not affected, but users cannot establish a new telnet session. Telnet access is permitted only from the IP address from where the CLI was entered and access granted through password authorization.

Telnet continues to require userid and password entry that is distinct from ipbxctl password access. However, unlike the ShoreWare CLI command and password, Telnet transmits the userid and password in the clear. Therefore, ShoreGear continues using the userid of “anonymous” and password of “ShoreTel” for initiating Telnet.

CLI passwords are configurable only through Director. The default password is ShoreTel.

Pressing the reset button on the switch resets the password to the default value of ShoreTel. The password that was active on the switch prior to the hardware reset is restored when the switch is connected to the network and receives an update from ShoreWare.

To set the ShoreGear passwords, access the Edit Other Parameters panel by selecting ***Administration -> System Parameters -> Other*** from the ShoreWare Director menu.

4.2.4.2 Burnflash Utility

The following table summarizes the commands available using the burnflash utility.

Command	Description
burnflash -s <*Switch IP Address*>	Updates all bootrom areas.
burnflash -test -s <*Switch IP Address*>	Checks to see if burnflash command will work.

Table 4-4 Burnflash Commands

4.3 Diagnostics

4.3.1 Using the Switch Trunk Debugging Tools

The ShoreGear switches have two tools that are helpful in troubleshooting trunks.

- Trunk_debug_level is a switch setting that identifies trunk events from the switch's perspective. Since ShoreTel applications manipulate dialed digit strings for both incoming and outgoing calls, the trunk debugger is typically used to validate the traffic between the CO and the switch. The recommended trunk debug level is 4.

Step 1 Open a Telnet session and set debug on by typing:

```
trunk_debug_level=4
```

Step 2 When finished, turn off debug by typing:

```
trunk_debug_level=0
```

- The D channel monitor helps you monitor the D channel of a PRI span. To do this, turn on D channel monitor of the switches.

  ShoreTel recommends that you use a Telnet interface that is capable of capturing the output of the commands.

For IPBX switches, to turn on the D channel monitor:

Step 1 Open a Telnet session and type:

```
-> remConsoleConnect
-> remConsoleShell
```

Step 2 At the remCons> prompt, type:

```
remCons> pri_trace=10
remCons> pri_log=10
```

At this point, all D channel data is dumped to the screen.

Step 3 When you are finished capturing data, turn the monitor off by entering:

```
remCons> pri_trace=0
remCons> pri_log=0
```

Step 4 Exit the remote console shell by typing:

```
<cntrl>+d
```

Step 5 Exit the remote console by typing:

```
-> remConsoleDisconnect
```

For SG switches, to turn on the D channel monitor:

Step 1 Open a Telnet session and type:

Step 2 At the remCons> prompt, type:

```
-> pri_trace=4
-> pri_log=4
```

At this point, all D channel data is dumped to the screen.

Step 3 When you are finished capturing data, turn the monitor off by entering:

```
-> pri_trace=0
-> pri_log=0
```

4.3.2 Using VxWorks Command Line Interface

VxWorks provides a variety of useful tools and debuggers. This command line interface offers access to both standard VxWorks commands and ShoreTel commands. You can access the VxWorks interface by opening a Telnet session to a switch without invoking CLI.

You may also enter the VxWorks command line interface from a serial interface by entering the command `gotoshell` from the Shoreline> prompt. To return to CLI, enter the command `cliStart`.

Use caution when using the VxWorks interface; running commands can degrade performance on the switch. ShoreTel does not support changing or setting IP or other parameters using the VxWorks interface. Changes made using this interface may not be persistent and using it may cause unpredictable behavior in the system.

4.3.2.1 Commands Available Through VxWorks CLI

The following table summarizes the commands available through the VxWorks interface.

Command	Description	Notes
adm_debug_level	Logs admission control and bandwidth manager signal flow onto serial port.	=2 logs more diagnostics.
adm_diag_level	Logs admission control and bandwidth manager signal flow into IPBX log.	=2 logs more diagnostics.
arpShow and arptabShow	Displays the ARP table.	
autoReboot = 0	Turns the switch watchdog off to prevent rebooting after a catastrophic failure.	Use this command only when directed by ShoreTel Customer Support.
bigNvRamSetup	Erases switch's configuration in NvRam.	
bootChange	Changes the boot ROM parameters.	Use with caution.
cid_debug_level	Logs caller ID related information for extensions.	

Table 4-5 VxWorks CLI Commands

Command	Description	Notes
cliStart	Opens the ShoreTel command line interpreter (from a Telnet session) from serial ports only.	You must reboot the switch to return to the VxWorks interface.
config_status	Outputs the configuration records for the switch.	
DEBUG_LEVEL	Sets the ShoreSIP debugging flags.	Recommend using level 0xe00.
diagdCommands	Outputs full switch diagnostic information.	
dial_num_dump	Displays information about switch's off-system extension configuration.	
dn_plan_status	Displays information about the switch's dial plan.	
dnp_debug_level	Displays detail information (digit by digit) about dial plan access.	Recommend using level 1.
dtmf_debug	Displays RFC2833 for G729 related events.	Values can be 0 or 1 (default is 0).
DumpSB	Displays maximum PMCSW outputs.	
DumpSRAM	Displays Motorola 860 processor information.	For IPBX model switches only.
dumpUsedBw	Displays information about actual bandwidth used on individual calls/legs.	
etherMonBroadcast	Writes the ethernet broadcast messages to a .cap file in \inetpub\ftproot directory of the ShoreWare server that are not intended for that switch.	Recommend using level 1.
etherMonDump	Writes the ethernet trace information captured when using EtherMonStart. Writes to a .cap file in \inetpub\ftproot directory of the ShoreWare server controlling the switch. The .cap file name is ST-<lst 3 bytes of MAC-time-date>.cap.	
etherMonStart <bytes>	Bypes is the number of bytes of information you want to capture (for example, 10000000). Captures ethernet packets for trace purposes	This command consumes memory on the switch. Use `memShow` to determine available memory and never specify more than is available.
etherMonStop	Stops capturing ethernet packets.	
eval_adm_var	Displays information about switch's own bandwidth usage.	
eval_bwm_var	Displays information about total and available bandwidth.	
ext_bca_status	Displays active BCA calls along with call stack usage information.	To be run on switches hosting BCA extensions.
ext_cco_status	Displays information the switch's extension CCOs.	
ext_conf_status	Displays MakeMe conference port status.	
ext_debug_level1	Logs extension CCO configuration.	
ext_debug_level	Sets the extension debugging level.	Recommend using level 4.
ext_pg_status	Displays active pickup group calls.	To be run on the switches hosting PG extensions.

Table 4-5 VxWorks CLI Commands

Command	Description	Notes
fax_debug_level	Used to display fax-related events and processings such as tone detection, fax determination, and fax redirect.	Values can be 0 or 1 (default is 0).
fax_verbose	Used to display fax/silence detection, jitter buffer freezing. and echo canceller disabling related events.	Values can be 0 or 1 (default is 0).
flsh_getVersion	Displays the firmware and bootrom versions for the switch.	
flsh_printBootLine	Prints the boot parameters of the switch.	
flsh_setBootSourceFlash	Sets the switch to boot from flash memory.	Requires a restart for changes to take effect.
flsh_setBootSourceFTP	Sets the switch to boot from FTP.	Requires a restart for changes to take effect.
g729_verbose	Displays more information for G729 calls.	Enable this for G729 calls with mscmd_verbose
hostShow	Displays the known hosts.	
hunt_load_debug	Logs basic huntgroup call flow.	Useful for debugging issues found during heavy call load.
icmpstatShow	Displays ICMP statistics.	
ipdt_debug_filter	Assuming two extensions in the system: Ext A and Ext B. To print out IPDT log for Ext A. > ipdt_debug_level = -1 > ipdt_debug_filter=1 (tell IPDT that we enable filter) > ipdt_restrictTraceExts "Ext A's#" (turn on log for Ext A) > ipdt_remRestrictTraceExt "Ext A's #" (turn off log for Ext A). To print log for all extensions: > ipdt_debug_filter =0	
ipdt_debug_level	Recommend setting to **= -1** to turn on all loggings.	
ipdt_dumpCCOCK	Dumps BB call key state, since there is no extension associated with BB.	
ipdt_dumpExtCalls	Dumps call information in the extension (e.g. callID, legID, call state and leg state, etc.)	
ipdt_dumpExtDisplay	Dumps the current display view from IPDT.	
ipdt_dumpExtensions	Dumps information for all extensions controlled by the switch and the information for monitored extensions and MAE (BCA) extensions that are in the same switch and in the different switches.	
ipdt_dumpExtCK	Dumps information for call keys on the extension. Useful for troubleshooting LED patterns and icon issues.	
ipdt_resetExtDisplay	Redisplay on the extension. If the phone display and IPDT display (ipdt_dumpExtDisplay) are desynchronized, we can run ipdt_reset_ExtDisplay to synchronize them.	

Table 4-5 VxWorks CLI Commands

Command	Description	Notes
ipdt_restrictTraceExts	Set ipdt_debug_filter to 1. Then, use ipdt_restrictTraceExts to turn on logging on a particular extension.	
ifShow	Displays the current configured network parameters.	
laa_debug_level	Logs backup auto attendant signal flow.	
lspConList	Displays switch connectivity to other switches.	
lsp_debug_level	Displays Location Service Protocol messages that are exchanged between switches.	Recommend using level 4.
lsp_ping	Tests the LSP UDP communication to the far end switch for 100 iterations.	example: -> lsp_ping "192.168.1.1",100 Tests LSP UDP communication to the far end switch at 192.168.1.1, for 100 iterations (nominally 1 second). If only the IP address is supplied, 1000 iterations (nominally 10 seconds) is used.
lspTelList	Displays local and remote contacts.	
lspTelList 1	Displays detailed information about local contacts.	
lspTelList 2	Displays detailed information about remote contacts.	
mae_debug_level	Logs BCA call flow information.	
mailbox_debug_level	Logs mailbox destination for a particular call.	
memShow	Shows current memory usage of the switch.	
mgcp_msg_debug	Logs MGCP messages.	
mgcp_trans_debug	Logs MGCP transactions.	
mohc_debug_level	Prints diagnostic information for music on hold calls when set to 1.	Can be set to either 0 or 1. Default is 0.
mpm_debug_mask=0x40	Sets mpm debug flag to output Caller ID information received on inbound calls.	
mpm_debug_mask=0x10	Displays detailed DTMF information.	
mpm_debug_mask=-1	Displays detailed mpm information. Full debug of inbound calls (CallerID, DTMF).	
mscmd_verbose	Prints diagnostic information for the media commands sent from Switch board layer when set to 1.	Main media command verbose variable. Default is 0.
msps	Displays media stream statistics for all active calls on the switch.	This is a helpful command for all media-related issues.
msps 7	Displays media stream statistics for active calls.	
msps 8	Displays media stream statistics.	Use only when directed by ShoreTel.
msps 16	Displays media stream statistics.	Use only when directed by ShoreTel.
mwi_debug_level	Logs message waiting indicator setting call flow.	

Table 4-5 VxWorks CLI Commands

Command	Description	Notes
ping "<*IP Address*>"		Include double quotes (“) around the IP address.
pri_log=4	Begins output of D-Channel information.	Must be in Remote Shell on IPBX model switches. (Recommend 4)
pri_trace=4	Sets the PRI D-Channel trace debug level.	Must be in Remote Shell on IPBX model switches. (Recommend 4)
pri_verbose	Traces a high level description of the PRI traffic sent and received by trunks on the switch.	Recommend setting pri_verbose=1
print_ether_stats	Prints the Ethernet statistics from the network controller.	
rdn_diag_level	Used to determine why calls are routing to particular destinations, similar to what gets put in the DRSMain log when DRS is enabled.	Useful values are 0 (none) or 5 (trace resolve_dn).
reboot	Reboots the switch.	
Record2File2(port,time,<file_name>;0)	Records inbound media on the specified port for the specified time (in seconds) and writers it to /inetpub/ftproot.	Writes to the TMS server controlling the switch. FTP write access must be enabled on the server.
rfc2833_for_g711_debug	Displays events related to RFC2833 for G711.	Default is 0. It is a bitmasked integer. Can be used as 1 and 2.
routeShow	Displays current routing table.	
routestatShow	Displays routing statistics.	
sb_debug_level	Switch board debug variable that prints debug information for the commands sent from Call control.	Useful values range from 1-5.
set_mpm_debug (char *)	Used to print information regarding commands/event interface between host CPU and DSPs.	Uses a string as a parameter (e.g. “pots”, “pstn”, “dtmfd”, “dtmfg”, “cdis”, “class”, “cpm” are valid parameters). Example: To print POTS related information, use set_mpm_debug(“pots”)
sip_debug_level=1	Logs ShoreSIP to SIP translation.	
sip_debug_level=2	Logs SIP messages also.	
sipuaCallList	Displays active SIP stack calls. sipuaCallList 2 dumps more call related information.	To be run on switches hosting SIP trunks/ extensions.
sipuaList	Displays list of SIP trunk/extension user agents.	To be run on switches hosting SIP trunks/ extensions.
t2t_debug_level	Logs trunk interval information like silence, trunk name, trunk state, etc.	
tcpstatShow	Displays TCP statistics.	
trans_debug	Logs ShoreSIP transactions.	

Table 4-5 VxWorks CLI Commands

Command	Description	Notes
traceroute "<*IP Address*>"	For troubleshooting network by mapping route packets use to traverse an IP network.	Remember to include double quotes (“) around the target IP address. (See Section 4.3.2.4 on page 65 for details.)
trunk_cco_status	Displays information about switch's trunk CCOs.	
trunk_debug_level	Sets the trunk debugging flag	Recommend using level 4.
uaCallList	Displays information about active calls and legs.	
ua_call_status	Shows a snapshot of the active call status of the switch.	
uaList	Displays list of ShoreSIP extension/trunk user agents.	
unset_mpm_debug(char*)	To disable **set_mpm_debug** command	
udpstatShow	Displays UDP statistics.	

Table 4-5 VxWorks CLI Commands

4.3.2.2 Creating an Ethernet Trace File Using a ShoreGear Switch

You can capture the output of VxWorks “ether” commands from the ShoreGear switches in an Ethernet Trace file that will be stored on the server that is managing that switch. To do so, follow the procedure below:

Step 1 Open a Telnet session and type:

```
memShow
```

Run this command to verify that the switch has at least 1 MB of memory to perform the procedure.

Step 2 From the **Start** menu, navigate to the **Control Panel** > **Administrative Tools** and locate the IIS Manager.

Step 3 Right-click on the IIS Manager and select **Properties**. Then, enable the ability to write to the FTP server by selecting the **Write** checkbox and clicking **OK**.

This enables the ability to write to the following directory: C:\Inetpub\ftproot

Step 4 At the command prompt, run the following VxWorks commands. (See the table on Table 4-5 on page 59 for more information about the specific commands.)

```
etherMonStart 1000000
```

Do not exceed 6 zeros!

```
etherMonStatus
etherMonBroadcast
etherMonDump
etherMonStop
```

At this point, all data from running these commands is stored in the file **_.cap** on **C:\Inetpub\ftproot**

Step 5 When you are finished capturing data, the file can be processed using an Ethernet packet analyzer, such as Ethereal or WireShark.

4.3.2.3 Recording Audio from a Physical ShoreGear Switch Port

You can capture audio output from a ShoreGear Switch physical port (e.g. trunk port) using VxWorks commands. Audio output is saved on the HQ or DVM server that controls the switch. To do so, follow the procedure below:

Step 1 From the **Start** menu, navigate to the **Control Panel > Administrative Tools** and locate the IIS Manager.

Step 2 Right-click on the IIS Manager and select **Properties**. Then, enable the ability to write to the FTP server by selecting the **Write** checkbox and clicking **OK**.

This enables the ability to write to the following directory: C:\Inetpub\ftproot

Step 3 At the command prompt, run the following VxWorks commands. (See the table on Table 4-5 on page 59 for more information about specific VxWorks commands.)

```
Record2File2 (1, 60, "test")
```

Audio data from running this command is stored in the file **test_rx.pcm** and file **test_tx.pcm** in **C:\Inetpub\ftproot**

When you are finished capturing data, a "PCM Raw Data" file is created with the following format profile: **8000 Hz**, **16-bit**, **Mono** and can be listened to using a standard application, such as "Adobe Audition."

4.3.2.4 Using the Traceroute Command from a ShoreGear Switch

The traceroute command offers a useful troubleshooting tool that determines the route taken by packets as they traverse an IP network from a ShoreGear switch to a specified destination. The command sends IP packets across the network, and the successive batches of packets have increased TTL (time-to-live) values.

TTL is a packet variable that defines the number of "hops" (stations) that a packet can pass through before it expires. When a station receives a packet that has expired, it discards the packet and sends a time exceeded message to the originating station. The traceroute command uses these expiration messages to build the path map.

By determining the path to a known destination, network technicians can identify firewalls blocking access to a site and gather information about the structure of a network and the IP address ranges associated with a host.

The traceroute command can be executed from the switch's command line or from *ipbxctl.exe* utility.

To run the traceroute command from the ShoreGear CLI, follow the procedure below:

Step 1 Open a Telnet session and type:

```
traceroute "IP address"
```

IP address is the address of the target destination and is a mandatory parameter. It must be in double-quotation marks.

Step 2 Press Enter.

Traceroute displays information about the number of hops, host IP addresses, and the amount of time required for each hop, as shown in Figure 4-1.

Table 4-6 lists the parameters that can be use with the traceroute command when executing the command from the ShoreGear switch's command line:

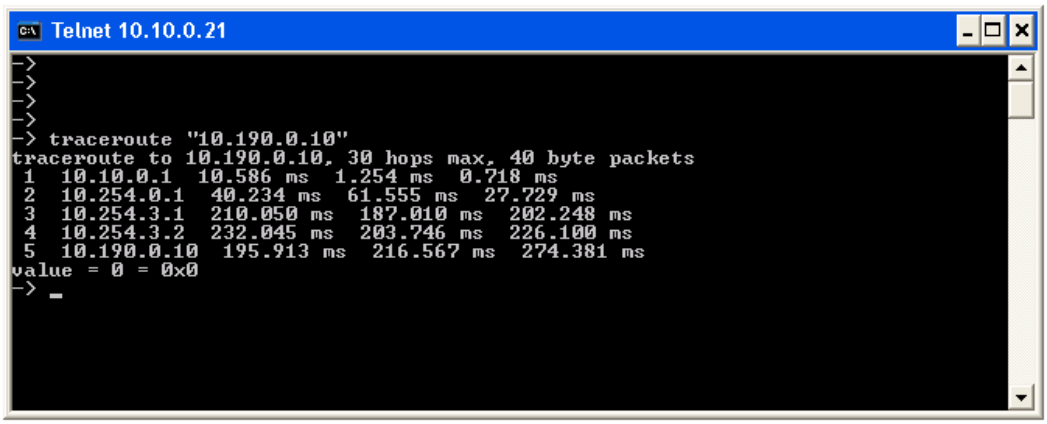

Figure 4-1 Output from Traceroute Command

Parameter	Description
"target IP address"	This parameter specifies the target IP address of the traceroute. This parameter is mandatory. IP addresses must be used and surrounded by quotes. DNS names are not supported.
-C	Probe on ShoreTel call control (ShoreSIP) port, using a ShoreSIP Request message, to determine if the packets flow from the switch through the network. This parameter uses fixed ports and version compatibility among all ShoreWare switches receiving packets.
-e	This parameter specifies the use of a fixed destination port and an incrementing source port. By default, traceroute increments the destination port with each probe. This port number is then used as a sequence number for matching packet responses to the probes. Incrementing the destination port number may complicate troubleshooting when packets are being filtered or lost at certain ports.
-I	This parameter specifies the ICMP protocol. (UDP is the default protocol used for traceroute.)
-S	This parameter specifies that probes are sent with a SIP message on the SIP destination port. Set this parameter to determine if SIP is flowing from the switch through the network. This parameter uses fixed ports.
-m <max_ttl>	*max_ttl* specifies the maximum time to live (TTL) value for traceroute packets. The default maximum TTL value is 30 bytes. Valid max_ttl values range from 1 to 255.
-f <first_ttl>	*first_ttl* specifies the TTL value of initial traceroute packets. The default initial TTL value is 1. Valid settings of first_ttl range from 1 to 255 and must be less than max_ttl.
-l <length>	*length* specifies the size of traceroute packet. The default packet size is 40 bytes. Valid length settings range from 100 to 1992.
-p <port>	*port* specifies the port for the destination probe. Valid port settings range from 1 to 65535.
-q <nqueries>	*nqueries* specifies the number of queries execute with each TTL value. The default value is 3. All integers greater than 0 are acceptable nqueries values.
-t <tos>	*tos* specifies Type of Server (tos) bit settings in the IP header of traceroute packets. The default value is 0. Valid tos settings range from 0 to 255.

Table 4-6 Traceroute Parameters

Parameter	Description
-w <waittime>	*waittime* specifies the period (seconds) a switch waits for a reply to a traceroute packet. The default value is 5 (seconds). Valid waittime settings range from 2 to 86400.
-z <pause>	*pause* specifies the period (milliseconds) between successive probes sent by the command. The default value is 0 (milliseconds). Valid pause settings range from 0 to 3600000.
Entering *traceroute* without listing any parameters returns the list of available parameters.	

Table 4-6 Traceroute Parameters

Sample syntax:

traceroute "target IP address", "[-CeIS] [-m <max_ttl>] [-f <first_ttl>] [-l <length>] [-p <port>] [-q <nqueries>] [-t <tos>] [-w <waittime>] [-z <pausemsecs>]"

4.3.3 Connecting to a ShoreGear Voice Switch

ShoreGear Half-Width and Full-Width voice switches provide a serial communications port accessible through a straight-through 9-pin serial cable.

To connect to a ShoreGear switch through a serial communications port:

Step 1 Connect a serial cable between a personal computer and the ShoreGear switch.

Step 2 Use a terminal emulation program such as HyperTerminal to open a connection to the switch.

Step 3 Apply these values to the terminal settings:

- Speed: 19.2 Kbs
- Data bit: 8 bits
- Stop bit: 1
- Parity: No parity
- Flow Control: None

4.3.4 Power over Ethernet Switches

When considering the use of Power over Ethernet (PoE) data switches in your network, keep in mind that not all PoE data switches provide power to all data ports, and not all PoE data switches provide adequate power to support all devices.

Model	Idle	Maximum	PoE Class
IP110	2.8 W	4.1 W	2
IP115	2.6 W	3.7 W	2
IP210	3.0 W	4.7 W	2
IP212k	3.0 W	5.0 W	2
IP230	2.9 W	4.4 W	2
IP265	3.5 W	5.9 W	2
IP530	3.1 W	5.9 W	2
IP560	3.3 W	6.4 W	2

Table 4-7 Power usage and class of ShoreTel IP Phones:

Model	Idle	Maximum	PoE Class
IP560g	4.1 W	7.1 W	3
IP565g	4.2 W	6.9 W	3
BB24	2.9 W	11.5 W (with IP560 connected)	3

Table 4-7 Power usage and class of ShoreTel IP Phones:

For example, when 24 IP560 phones are plugged into a switch, the maximum power requirement could reach 153.6 W (24 phones x 6.4W/phone).

- The value in the **Maximum** column in Table 4-7 is normally a spike – typically during bootup. During normal operation, phones require less power.
- Verify power allocated to the PoE ports matches the switch wattage.
- ShoreTel recommends selecting a PoE data switch that has "4 hardware queues" for Quality of Service (QoS) to ensure that rules can be set up to ensure adequate bandwidth for VoIP and other critical traffic.

CHAPTER 5

Voicemail Model Switches

5.1 Introduction

Voicemail Model Switches are ShoreGear switches that provide voicemail services and access to auto attendant menus for extensions hosted by the switch. Voicemail Model (V Model) switches provide local access to voicemail while being controlled by a Distributed server at a different location.

Voicemail Model switches store voicemail in Compact Flash (CF) cards. Auto Attendant menus, greetings, and prompts, are stored in permanent flash memory. Voicemail backup and restore routines are available through Director for protecting voice mail on a regular basis. If a switch is disabled, information on the Compact Flash is retained and can be moved to another switch of the same model.

V Model switches are deployed in the same manner as other ShoreGear 1-U Half Width switches and managed similarly to other switches and servers. Director windows configure switch, voicemail, and server settings. Device status is also monitored through Director maintenance windows.

Three ShoreGear switches that operates as a ShoreGear voice switch and as a voice mail server:

- ShoreGear 90V
- ShoreGear 90BRIV
- ShoreGear 50V

5.2 Utilities

5.2.1 Accessing Voicemail Model Switch Utilities

ShoreGear switch utilities are accessible through the Maintenance port, an SSH client, or an MS windows program executed from a command prompt on the Main or a Distributed server. The following sections describe utility access methods.

For security purposes, the Switch accepts requests from only CLIs s running on the local host, the controlling Distributed server, or the Main ShoreTel server.

5.2.1.1 Accessing Utilites from the Serial Port

Switch utilities and the UBOOT boot loader are accessible through the maintenance port located on the faceplate. The available utility depends on the state of the switch at the time of access.

- During normal switch operation, the Maintenance port provides access to a specified Linux shell. By default, STCLI is the specified shell.

- During a switch boot, UBOOT is accessed by typing a key immediate after the autoboot.

To access ShoreGear utilities through the Maintenance:

Step 1 Connect a serial cable between a personal computer and the ShoreGear switch.

Step 2 Use a terminal emulation program, such as Tera Term Pro freeware, to open a connection to the switch.

Step 3 Apply these values to the terminal settings:

- Speed: 19.2 Kbs
- Data bit: 8 bits
- Stop bit: 1
- Parity: No parity
- Flow Control: None

Refer to utility descriptions for access information through the Maintenance port.

5.2.1.2 Accessing Utilities from SSH

ShoreTel provides access to several Voicemail Model utilites through a Linux BASH command line. Voicemail Model switches define two accounts:

- **Admin:** The admin account provides access to selected ShoreTel and Linux utilities, including all Voicemail Model command line interfaces. ShoreTel recommends that user log into the Admin account when accessing Linux utilities.

  Logging into the Admin account immediately opens the STCLI interface.

- **Root:** The root account provides access to all ShoreTel and Linux utilities. Access to this account should be resticted because of the potential for creating unintended switch problems.

  Logging into the Root account immediately opens a Linux BASH shell.

Access to the Linux BASH command line through an SSH client. Free SSH clients, such as PuTTY, are avaliable through the internet.

To access a Linux BASH Shell account:

Step 1 Open a SSH client access panel.

Figure 5-1 displays the PuTTY Configuration panel.

Step 2 Open the command line by entering the IP address of the switch to which the command line will access in the appropriate data entry field, then pressing the button that activates the command shell.

In Figure 5-1, the IP address is placed in the Host Name (or IP address) field, after which pressing the Open button opens the command line interface.

Step 3 Enter the username of the desired account on the command line, then press Enter key.

In Figure 5-1, admin is the specified account.

The command line response depends on the account to which you log into. When logging into admin, the CLI open STCLI. when logging into the Root account, the CLI displays a prompt that displays root as the account.

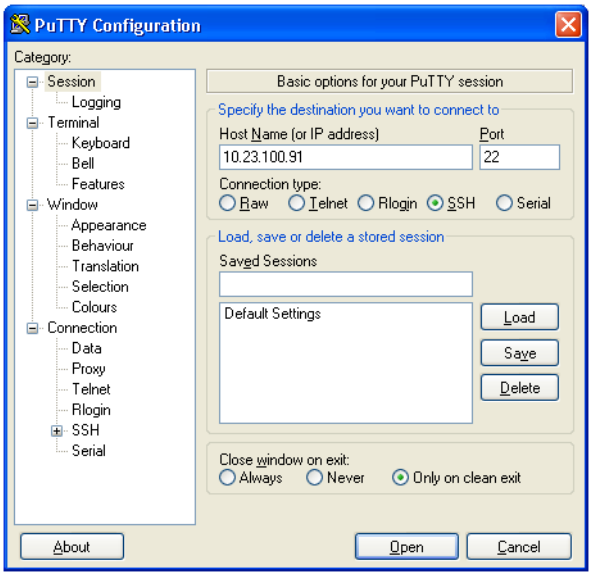

Figure 5-1 PuTTY Configuration panel

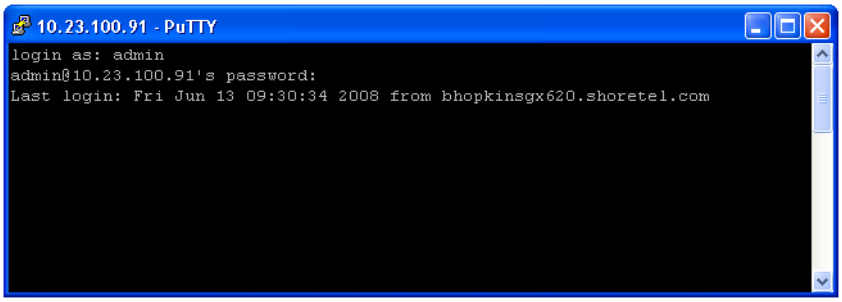
10.23.100.91 - PuTTY
login as: admin
admin@10.23.100.91's password:
Last login: Fri Jun 13 09:30:34 2008 from bhopkinsgx620.shoretel.com

Figure 5-2 PuTTY Command Prompt window

5.2.1.3 Accessing Utilities from an MS Windows Server

Headquarters and distributed services contain executable files that access Voicemail model switches. On a normally installed server, utility commands are located at *C:\Program Files\Shoreline Communications\ShoreWare Server*. Commands that you can perform from a server through MS windows include:

- svccli – refer to Section 5.2.3.1
- burnflash – refer to Section 5.3.3.4
- ipbxctl – refer to Section 5.2.2.4

To run ShoreGear switch utilities through MS Windows:

Step 1 Open a command prompt by pressing the Start button and selecting *Program -> Accessories -> Command Prompt*

Step 2 Enter the name of the utility on the command line, using the IP address of the Voicemail Model switch as the switch parameter, then press the Enter key.

The location of these utilities is:

```
C:\Program Files\Shoreline Communications\ShoreWare Server
```

5.2.2 Switch Utilities

A set of command line interface (CLI) commands supports various operations. The commands to backup and restore voicemail, stop or start services and groups, format and CF cards, among other operations.

5.2.2.1 UBOOT

UBOOT is the boot loader for Voicemail Model switches. The UBOOT environment is accessed from a terminal emulator through the serial port when the switch is booted. Before starting the boot, UBOOT lists the CPU characteristics and displays results of the POST. The switch then waits a specified period before starting the autoboot; you can modify the duration of this period through an SVCCLI command; the default period is three seconds.

To stop the autoboot during this delay, press any key. After the autoboot is stopped, you can display and change booting variables.

The command **printenv** displays all booting shell variable settings. The following is a typical response to executing printenv:

```
bootdelay=3
serial#=50VJ0724081DFA
ethaddr=00:10:49:08:1d:fa
ipaddr=10.1.4.0
netmask=255.255.0.0
gatewayip=10.1.0.1
serverip=10.1.1.255
user=anonymous
pass=tsk
bootfile=/tskl/uImage
autoload=FTP
bootcmd=dhcp;bootm
flags=0x40
```

These settings are edited through the **setenv** command. The **setenv** command has the format setenv <variable> <value>.The **saveenv** command saves environment variable settings to the non-volatile memory on the switch. Execute saveenv after the variables are set to the required values. Refer to Section 5.5.5 for a description of UBOOT commands.

Boot flags control switch operations after startup. Refer to Section 5.5.5 for a description of UBOOT flag values.

5.2.2.2 STCLI

STCLI, also known as the ShoreTel Shell, displays and modifies system configuration parameters. You can implement static or dynamic IP addressing for the switch from STCLI. You can also reboot the switch from STCLI. Figure 5-3 diplays the STCLI prompt. The main STCLI menu appears below the ShoreTel logo.

To open STCLI:

- Access the Maintenance port, as described in Section 5.2.1.1. If window displays the Linux prompt, enter STCLI on the command line.
- Access the SSH and log in as the administrator, as described in Section 5.2.1.2.

Exiting STCLI returns the user to the Admin account BASH shell. To close the window, type Exit on the Linux command line.

STCLI commands are described in Section 5.5.1.

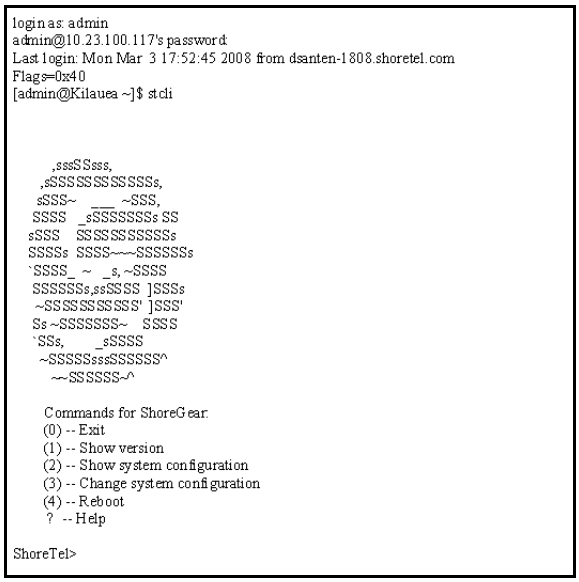

Figure 5-3 STCLI Login and Main Menu

5.2.2.3 CLI

The CLI interface accesses diagnostic tools, manipulates debug setting levels, and displays system information.

Section 5.5.3 describes CLI commands.

For security purposes, the Services Manager accepts requests from only a CLI that is running on the local host, the controlling Distributed server, or the Main ShoreTel server.

- To access CLI, open a Linux BASH shell, as described in Section 5.2.1, and enter CLI at the prompt.
- To exit CLI, type **Ctrl-c** or enter the letter **q** at the CLI prompt.
- To view a list of CLI variables and their current values, enter **variables** on the command line.
- To view the current value of a variable, enter that variable name on the command line

  To manually change the value of the variable, enter the variable name and new value on the command line.
- To specify the destination of switch trace information, enter the following on the command line:
  - — ***redirect 0*** trace information sent to the the Mainentance port.
  - — ***redirect 1*** trace information is sent to the current device.

5.2.2.4 ipbxctl

ipbxctl commands perform switch control and diagnostic tasks, including switch rebooting, clearing flash memory, and running traceroute.

ipbxctl is run as a windows program from the Main Server or the controlling Distributed Server, as described in Section 5.2.1.3

Section 5.5.7 describes ipbxctl commands.

5.2.2.5 regedit

Regedit, a ShoreTel utility that modifies Registry-type data structures in the switch, is accessible through the Root account.

V Model Switches have a Registry similar to Windows Servers. The Registry is a ShoreTel construct, not part of Linux. To edit the Registry, log in as root and run the RegEdit command line tool from the bash shell. RegEdit may be used to change logging levels on applications and set other parameters that change their behavior.

Section 5.5.8 describes regedit commands

5.2.3 Server Utilities

5.2.3.1 SVCCLI

The SVCCLI commands control low level switch parameter settings and application commands, including Compact Flash storage, switch password, and service control operations.

Section 5.5.2 describes SVCCLI commands.

For security purposes, the Services Manager accepts requests from only a CLI that is running on either the local host, the controlling ShoreTel server, or the headquarters (HQ) ShoreTel server.

- To access SVCCLI, perform one of the following:
  - — Open a Linux BASH shell, as described in Section 5.2.1, and enter SVCCLI at the prompt.
  - — Run SVCCLI from the Main Server or a Distributed Server, as described in Section 5.2.1.3
- To display the SVCCLI commands, enter **help** or **?** at the SVCCLI prompt.
- To exit SVCCLI, type **Ctrl-c** or enter the letter **q** at the SVCCLI prompt.

5.2.3.2 cfg Utility

The **cfg** utility is a command-line tool that provides detailed information about the voice mail application.

Cfg.exe can be found in the ***\shoreline communications\shoreware server*** directory.

To start cfg:

Step 1 Open a DOS window pointing to the ***\shoreline communications\shoreware server*** directory.

Step 2 Enter `cfg` and press Enter.
When you see the prompt `/*Local*//->,` cfg is ready.

All commands are entered at the above prompt. Results are displayed in the DOS window or in the voice mail logs.

WARNING Some **cfg** utility commands may damage the system if used incorrectly. Make sure you understand the commands before you use them.

Section 5.5.4 lists the commands available through the cfg utility.

5.3 Booting and Restarting

5.3.1 Description

Rebooting and ***restarting*** V model switches have different scopes.

- Rebooting a V model switch also reboots the Linux kernel and everything that a kernel reboot entails.

  A reboot takes much longer than a restart.

- Restarting a V model switch only the reboots the ShoreGear application layer.

  On ShoreGear switches running on VxWorks, rebooting and restarting are identical.

Under certain conditions, initiating a restart will reboot the switch. One example is when a switch upgrade is available.

When a ShoreGear voice switch boots, it requires an IP address to connect to the network and an application program. ShoreGear voice switches are set to use a DHCP server for an IP address and to retrieve the application from the switch's flash memory.

If a DHCP request receives no response, the switch tries a BootP request as a backup. ShoreTel recommends using static IP parameters configured via the serial port, as this is much more reliable. When using DHCP, ShoreTel recommends using DHCP reservations for each switch to ensure that DHCP leases are not lost.

If a DHCP server is not available, you can set the IP address manually from the switch's maintenance port from STCLI.

If the switch fails to load the application from flash and does not have the IP address of the ShoreWare server, you can set the IP address and boot parameters by connecting to the maintenance port and using the configuration menu. The configuration menu allows you to set the IP address of the switch and enter the ShoreWare server (boot host) IP address.

A V model switch can be brought up by a regular (flash memory-sourced) boot or by a software upgrade boot.

5.3.2 Specifying a Static IP Address

V Model switches normally use DHCP to dynamically set the device IP address and specify the addresses of the servers to which it communicates. Switches are set into fixed address mode through CLI instructions.

The following procedure places the V Model switch into fixed address mode:

Step 1 Access the STCLI command line interface, as described in Section 5.2.2.2 on page 72.

Step 2 Enter "3" on the command line to select **Change System Configuration**.

The CLI window displays the Change System Configuration options.

Step 3 Enter "6" on the command line to select Enable/Disable DHCP/BOOTP

The CLI window displays the DHCP/BOOT options.

Step 4 Enter "0" on the command line to select Manual Configuration.

Step 5 Change the network parameters as required to support the fixed address from the Change System Configuration entry line.

Step 6 After completing changes to the configuration, type Exit to close the CLI.

Step 7 Reboot the switch.

5.3.3 Reboot Methods

5.3.3.1 Flash Boot

The standard method for booting a ShoreGear voice switch is to boot from the switch's flash memory. When a ShoreGear switch is first powered on, it reads the boot parameters stored on the boot ROM, which instructs the switch to load software from flash memory. When the software starts, it loads its configuration, which is also stored in flash memory.

5.3.3.2 Default Button

The Default Button is the small "paperclip" button on the switches. Pressing this button will invoke scripts that will overwrite the contents of the NAND flash with the contents from the FTP Server. The contents of the Compact Flash are untouched.

Pressing this button and holding for 10 seconds will also reformat the Compact Flash.

5.3.3.3 FTP Boot

Booting from FTP is available for instances when you cannot boot the switch from flash memory. When you boot a switch from FTP, the operating system and software load from the FTP site identified in the boot parameters. The loaded configuration is a configuration received from the TMS server.

Voicemail services on the switch are disabled after booting from FTP and are restarted only by booting from Flash. After an FTP boot, the switch can perform telephony functions as those available through other ShoreGear switches.

FTP boot on a V model switch is used for troubleshooting. FTP boot can also support certain maintenance tasks and the backup and restore facilities. However, a V model switch that has been booted by way of FTP cannot run voicemail: it can operate only as a voice switch (controlling phones, trunks, and call routing).

5.3.3.4 Burnflash

Burnflash forces a reboot and install new software.

The **burnflash** command burns a ShoreTel image to the CF card. It unconditionally replaces the resident image and then reboots the system, but it does not destroy any voice mail. The purpose of burning the image to the CF is to enable the switch to boot from NAND flash memory rather than to do an FTP boot from the server. (FTP boot supports certain maintenance functions, such as an emergency boot if the flash becomes damaged. FTP boot is not what a user should use to boot the switch because this action does not support certain services. For example, an FTP boot does not mount the CF file system, so voice mail would not be running after an FTP boot.)

If a user created a static configuration for IP addresses and other system parameters through the STCLI (option 3), those parameters must be reconfigured after **burnflash** runs.

5.4 Diagnostics and Repair

5.4.1 Using Switch Trunk Debug Tools

Trunk_debug_level is a switch setting that identifies trunk events from the switch's perspective. Since ShoreTel applications manipulate dialed digit strings for both incoming and outgoing calls, the trunk debugger is typically used to validate the traffic between the CO and the switch. The recommended trunk debug level is 4.

Step 1 Access the CLI shell, as described in Figure 5.2.2.3.

Step 2 Enter the following command:

```
trunk_debug_level=4
```

Step 3 When finished, turn off debug by typing:

```
trunk_debug_level=0
```

- The D channel monitor helps you monitor the D channel of a PRI span. To do this, turn on D channel monitor of the switches.

  ShoreTel recommends using an SSH interface that is capable of capturing the output of the commands.

5.4.2 Creating an Ethernet Trace File

You can capture the output of "ether" commands from the ShoreGear switches in an Ethernet Trace file stored on the server that is managing that switch. To do so, follow the procedure below:

Step 1 Access the CLI shell, as described in Figure 5.2.2.3.

Step 2 Enter the following command:

```
memShow
```

Run this command to verify that the switch has at least 1 MB of memory to perform the procedure.

Step 3 From the **Start** menu, navigate to the **Control Panel** > **Administrative Tools** and locate the IIS Manager.

Step 4 Right-click on the IIS Manager and select **Properties**. Then, enable the ability to write to the FTP server by selecting the **Write** checkbox and clicking **OK**.

This enables the ability to write to the following directory:
C:\Inetpub\ftproot

Step 5 At the CLI prompt, run the following commands. (See the table on Table 5-2 on page 87 for more information about the specific commands.)

```
etherMonStart 1000000;                    Do not exceed 6 zeros!
etherMonStatus
etherMonBroadcast
etherMonDump
etherMonStop
```

At this point, all data from running these commands is stored in the file **_.cap** on **C:\Inetpub\ftproot**

Step 6 When you are finished capturing data, the file can be processed using an Ethernet packet analyzer, such as Ethereal or WireShark.

5.4.3 Recording Audio from a Switch Port

You can capture audio output from a ShoreGear Switch physical port (e.g. trunk port) using a CLI command. Audio output is saved on the HQ or DVM server that controls the switch. To do so, follow the procedure below:

Step 1 From the **Start** menu, navigate to the **Control Panel** -> **Administrative Tools** and locate the IIS Manager.

Step 2 Right-click on the IIS Manager and select **Properties**. Then, enable the ability to write to the FTP server by selecting the **Write** checkbox and clicking **OK**.

This enables the ability to write to the following directory:
C:\Inetpub\ftproot

Step 3 At the CLI prompt, run the following command:.

```
Record2File2 (1, 60, "test")
```

Audio data from running this command is stored in the file **test_rx.pcm** and file **test_tx.pcm** in **C:\Inetpub\ftproot**

When you are finished capturing data, a "PCM Raw Data" file is created with the following format profile: **8000 Hz**, **16-bit**, **Mono** and can be listened to using a standard application, such as "Adobe Audition."

5.4.4 Using Traceroute

The traceroute command offers a useful troubleshooting tool that determines the route taken by packets as they traverse an IP network from a ShoreGear switch to a specified destination. The command sends IP packets across the network, and the successive batches of packets have increased TTL (time-to-live) values.

TTL is a packet variable that defines the number of "hops" (stations) that a packet can pass through before it expires. When a station receives a packet that has expired, it discards the packet and sends a time exceeded message to the originating station. The traceroute command uses these expiration messages to build the path map.

By determining the path to a known destination, network technicians can identify firewalls blocking access to a site and gather information about the structure of a network and the IP address ranges associated with a host.

The traceroute command can be executed from the switch's command line or from *ipbxctl.exe* utility.

To run the traceroute command from the ShoreGear CLI, follow the procedure below:

Step 1 Access the CLI shell, as described in Figure 5.2.2.3.

Step 2 Enter the following command:

```
traceroute "IP address"
```

IP address is the address of the target destination and is a mandatory parameter. It must be in double-quotation marks.

Step 3 Press Enter.

Traceroute displays information about the number of hops, host IP addresses, and the amount of time required for each hop.

Table 5-1 lists the parameters that can be use with the traceroute command when executing the command:

Parameter	Description
"target IP address"	This parameter specifies the target IP address of the traceroute. This parameter is mandatory. IP addresses must be used and surrounded by quotes. DNS names are not supported.
-C	Probe on ShoreTel call control (ShoreSIP) port, using a ShoreSIP Request message, to determine if the packets flow from the switch through the network. This parameter uses fixed ports and version compatibility among all ShoreWare switches receiving packets.
-e	This parameter specifies the use of a fixed destination port and an incrementing source port. By default, traceroute increments the destination port with each probe. This port number is then used as a sequence number for matching packet responses to the probes. Incrementing the destination port number may complicate troubleshooting when packets are being filtered or lost at certain ports.
-I	This parameter specifies the ICMP protocol. (UDP is the default protocol for traceroute.)
-S	This parameter specifies that probes are sent with a SIP message on the SIP destination port. Set this parameter to determine if SIP is flowing from the switch through the network. This parameter uses fixed ports.
-m <max_ttl>	*max_ttl* specifies the maximum time to live (TTL) value for traceroute packets. The default maximum TTL value is 30 bytes. Valid max_ttl values range from 1 to 255.
-f <first_ttl>	*first_ttl* specifies the TTL value of initial traceroute packets. The default initial TTL value is 1. Valid settings of first_ttl range from 1 to 255 and must be less than max_ttl.
-l <length>	*length* specifies the size of traceroute packet. The default packet size is 40 bytes. Valid length settings range from 100 to 1992.
-p <port>	*port* specifies the port for the destination probe. Valid port settings range from 1 to 65535.
-q <nqueries>	*nqueries* specifies the number of queries execute with each TTL value. The default value is 3. All integers greater than 0 are acceptable nqueries values.
-t <tos>	*tos* specifies Type of Server (tos) bit settings in the IP header of traceroute packets. The default value is 0. Valid tos settings range from 0 to 255.
-w <waittime>	*waittime* specifies the period (seconds) a switch waits for a reply to a traceroute packet. The default value is 5 (seconds). Valid waittime settings range from 2 to 86400.
-z <pause>	*pause* specifies the period (milliseconds) between successive probes sent by the command. The default value is 0 (milliseconds). Valid pause settings range from 0 to 3600000.
Entering *traceroute* without listing any parameters returns the list of available parameters.	

Table 5-1 Traceroute Parameters

Sample syntax:

traceroute "target IP address", "[-CeIS] [-m <max_ttl>] [-f <first_ttl>] [-l <length>] [-p <port>] [-q <nqueries>] [-t <tos>] [-w <waittime>] [-z <pausemsecs>]"

5.4.5 Reformatting the Compact Flash

V model switches use the Ext3 file system on the CF card. (Therefore, with software on a PC that can read Ext3 files, the user can plug the CF card into a PC and access the voicemail.)

The CF is not hot swappable; you must shut down the switch to remove the card.

To format the compact flash:

Step 1 Open SVCCLI

Step 2 Enter formatcf on the command line.

5.5 Reference

5.5.1 STCLI Command Descriptions

The following lists STCLI commands. Refer to Section 5.2.2.2 for a description of STCLI.

- **Option 0**

  To exit the main menu of STCLI and return to the Linux prompt, a user enters a 0 at the STCLI prompt. Because 0 can be an option for some parameter settings, it does not always work as an escape. In these situations, a Ctrl-c also triggers an exit from STCLI and a return to the Linux prompt.

  A user must exit STCLI before being able to start up the SVCCLI.

- **Option 1**

  To see the version of system software running on the current V model switch, enter a 1 at the STCLI.

- **Option 2**

  To see current values for the system parameters that are viewable through STCLI, a user enters a 2 at the STCLI prompt. An example of the parameters appears in Figure 5-4. Of these parameters, the items that an administrator can change are described in Option 3.

```
ShoreTel> 2
Current system configuration:
Boot method                 = FLASH
Boot command                = jboot;bootm
Boot file                   = uImage
FTP user name               = anonymous
FTP password                = tsk
Ethernet address            = 00104907280A
IP address                  = 10.23.100.117
IP subnet mask              = 255.255.255.0
Server IP address           = 10.23.100.117
Gateway IP address          =
DNS IP address              =
Time server IP address      =
DHCP/BOOTP                  = DHCP enabled
Ethernet link               = auto-negotiate 100 Mb,
                                        full-duplex
Domain name                 =
```

Figure 5-4 Current System Configuration

- **Option 3**

  The system parameters that an administrator can specify through manual configuration are available through option 3 in the main menu, as shown in Figure 5-5. Figure 5-5 also illustrates the type of prompting that begins after a user selects a parameter to change. When a user selects a parameter to change, the prompt changes to show the mode to which the CLI has changed—"ShoreTel Config> 1"in Figure 5-5.

One very significant configuration decision is whether to enable DHCP or static IP address configuration. If the administrator chooses static (manual) configuration by disabling DHCP, then all parameters displayed by option 2 (that can be configured) must be manually configured through option 3. A static configuration is persistent and is preserved across upgrades. However, the configuration file is cleared if the SVCCLI **burnflash** command (or its equivalent ***upgrade 3***) is run, so static configurations must be recreated after either **burnflash** executes or ***upgrade 3*** is run.

If DHCP/BOOTP is enabled, the IP address of the network time protocol (NTP) server is provided.

To configure the system manually:

Step 1 Enter a 6 to select the DHCP/BOOTP enable

Step 2 Enter a 0 to specify manual configuration. (Otherwise, enter a 1 for DHCP or a 2 for BOOTP.)

```
ShoreTel> 3

        Change system configuration:
        (0) -- Return to previous menu
        (1) -- Change IP address
        (2) -- Change IP subnet mask
        (3) -- Change gateway IP address
        (4) -- Change server IP address
        (5) -- Change boot method
        (6) -- Enable/disable DHCP/BOOTP
        (D) -- Set/change domain name
        (P) -- Set/change primary DNS IP address
        (S) -- Set/change secondary DNS IP address
        (T) -- Set/change network time server IP address
         ?  -- Help

ShoreTel Config> 1
Current switch IP address is:  10.23.100.117
Enter new switch IP address
->
```

Figure 5-5 Configurable System Parameters

If the user enters configuration mode but wants to escape without making changes, the Ctrl-c sequence provides an escape that returns the user all the way to the Linux prompt. After entering configuration mode, the user should not enter 0 as an escape character because 0 is a configuration choice for different tasks in configuration mode.

- **Option 4**

  Option 4 is for rebooting the system. After entering a 4, the user sees a request for a confirmation to proceed with the reboot.

- **Help**

  Entering a ? lists the main menu items.

- ***Ctrl-c***

  Pressing Ctrl-c from any STCLI option state causes an exit from STCLI and a return to the Linux prompt.

5.5.2 SVCCLI Command Descriptions

The following is a list of SVCCLI commands. Refer to Section 5.2.2.2 for a description of SVCCLI.

- ? or **help**

  The ? or **help** command displays a list of all commands and the syntax of each. The command takes no parameters (such as an individual command name.) An example of the command output follows:

```
>?
usage is svccli [cmd [param]]
backupvm                                - backup voicemail files
burnflash                               - unconditionally replace flash
                                          images then reboot
chgrootpassword<password>               - change root password.
chguserpassword<password>               - change user password
disablegroup    <groupname> or *        - disable group of services
disablesvc      <servicename> or *      - disable services
dump                                    - dump ServicesMgr internal
                                          tables
enablegroup     <groupname> or *        - enable group of services
enablesvc       <servicename> or *      - enable services
erasecf                                 - erase all files from compact
                                          flash then reboot
flushlogs                               - tell services to flush logs
formatcf                                - format removable compact
                                          flash
getsvcstatus    <servicename> or *      - get service status
killsvc         <servicename> or *      - kill -9 services
q or ctrl-c                             - quit svccli
reboot[idle]                            - check upgrade, reboot machine
                                          [when switch is idle]
restart[idle]                           - restart services [when switch
                                          is idle]
restartgroup    <groupname> or *        - stop then start group of
                                          services
restartsvc      <servicename> or *      - stop then start services
restorevm                               - restore voicemail files from
                                          backup
sendcmd         <servicename>           - send command to service
setregistry     <hqipaddr> <ctlipaddr>- set ip addresses of servers
startgroup      <groupname> or *        - start group of services
startsvc        <servicename> or *      - start services
stopgroup       <groupname> or *        - stop group of services
stopmgr                                 - stop services manager
stopsvc         <servicename> or *      - stop services
Note: use "all" on the command line in place of "*"
```

Figure 5-6 SVCCLI Commands

At the bottom of its display, SVCCLI states that a command can apply to all available arguments by inclusion of "all" or "*." For example, the following SVCCLI entry would restart all services:

```
>restartsvc *
```

- **backupvm - Back up voice mail**: The **backupvm** command performs on-demand backup of voice mail, Auto-Attendant data, and the logs that are written to the CF card. On-demand backup begins immediately upon **backupvm** entry. During a backup, voice mail service continues, and an incoming voice mail is backed up if it was already being recorded when the backup began. When the backup finishes, the SVCCLI displays a message indicating it has finished. (In contrast, during a restore operation, the voice

mail server is stopped. Also, the restore operation can by started from the SVCCLI only.)

If automatic backup is disabled in the ShoreWare Director, **backupvm** still triggers the backup but only if backup has been configured in the Director.

Whether for a scheduled or an on-demand backup, pre-configuration of the backup target is necessary. For a description of how to configure an FTP server to be the target of the backup, see ShoreTel Administration Guide.

On-demand backup can serve a variety of purposes. These purposes are usually in response to anomalous situations. The main purpose of on-demand backup is to reduce the risk of losing voice mail if a damaged or faulty CF is suspected. For example, if the installation of a new CF card is immediately required, on-demand backup is the first step. After the new card is formatted, the **restorevm** command can bring the backed-up voice mail to the new card.

Run **getsvcstatus all** to see the state of the CF file system. At the bottom of the screen for this command's output, the state of each file system is shown. The following line is from the file system lines of the **getsvcstatus** output and shows that the CF file system is mounted.

```
/dev/kcfa1                    984871      268663      666163 29% /cf
```

If the"/cf "is missing, then the CF file system is not mounted, and remedial action is necessary. In this case, not only does voice mail have nowhere to go, but the logs cannot be stored on CF, so the system provides some space in RAM for holding the most important logs.

After backup, the suspect CF card can be removed and tested in another system, and a new card can be installed after voice mail is backed up.

- **burnflash - Burn flash:** The **burnflash** command burns a ShoreTel image to the CF card. It unconditionally replaces the resident image and then reboots the system, but it does not destroy any voice mail. The purpose of burning the image to the CF is to enable the switch to boot from NAND flash memory rather than to do an FTP boot from the server. (FTP boot supports certain maintenance functions, such as an emergency boot if the flash becomes damaged. FTP boot is not what a user should use to boot the switch because this action does not support certain services. For example, an FTP boot does not mount the CF file system, so voice mail would not be running after an FTP boot.)

  If a user created a static configuration for IP addresses and other system parameters through the STCLI (option 3), those parameters must be reconfigured after **burnflash** runs.

- **chgrootpassword - Change root password**: The **chgrootpassword** command changes the root password for accessing the ShoreGear CLI. Arguments for this command are old and new passwords. This password was created in the Director in the System Parameters –> Other window.

  Syntax: **chgrootpassword** <***password***>

- **chguserpassword - Change user password:** The **chguserpassword** command changes an administrator password for accessing the ShoreGear CLI. Arguments for this command are old and new passwords. This password was created in the Director in the System Parameters –> Other window.

  Syntax: **chguserpassword** <***password***>

- **disablegroup - Disable group:** The **disablegroup** command disables a group of services. Disabling means that one group or all groups of services are suspended but

not completely turned off. To enable any disabled groups, use the **enablegroup** command.

This command is primarily for trouble shooting. During normal operation, if a group of services fails, the system automatically tries to restart the stopped services. However, for troubleshooting purposes, it can be important for the group to remain inactive.

Syntax: **disablegroup** <***group name***> * or **all**

- **disablesvc - Disable service:** The **disableservice** command disables one or all services. Disabling means that a service is suspended but not completely turned off. To enable disabled services, use the **enableservice** command.

  This command is primarily for troubleshooting. During normal operation, if a service fails, the system automatically tries to restart any stopped services. However, for troubleshooting purposes, it can be important for the servive(s) to remain inactive.

  This status of the service(s) is shown in the output of the **getsvcstatus** command.

  Syntax: **disablesvc** <***service name***> * or **all**

- **dump - Dump: Dump** sends a dump command to certain services. This command is used by ShoreTel engineering for debug only. Typically, the **dump** command dumps a service's internal state to a log file. The **dump** command does not work on all services.

  Syntax: **dump** <***service name***>

- **enablegroup - Enable a group of services:** The **enablegroup** command enables one or more groups of services after they have been disabled by the **disablegroup** command. These two commands apply to troubleshooting.

  Syntax: **enablegroup** <***group name***> * or **all**

- **enablesvc - Enable service:** The **enablesvc** command enables one or more services after they have been disabled by the **disablesvc** command. These two commands apply to troubleshooting.

  Syntax: **enablesvc** <***service name***> * or **all**

- **erasecf - Erase CF:** The **erasecf** command completely erases all the contents of a CF card. Backing up the CF before using this command would probably be a wise move. Example purposes for erasing the CF could be:

  — To correct suspected memory corruption.

  — To erase a CF that is both formatted and mounted. (The **formatcf** command is not available for a CF card that is formatted and mounted.)

  After CF erasure, the system automatically reboots. The reason for rebooting is so that, when the system detects that the CF is empty, the system recreates the file structure and replaces all other voice mails and other needed elements on the CF card.

  Syntax: **erasecf**

- **flushlogs - Flush logs:** The **flushlogs** command is a utility that copies certain system logs to the CF card. In normal operation, the system performs very little logging. Only severe problems are logged to files on the V model switch. The logging system is implemented in a memory circular buffer to record the logs (and perform certain tracing tasks.) Each log file has its own circular buffer, and these circular buffers can be forced to a log file by the **flushlogs** command.

  Syntax: **flushlogs**

- **formatcf - Format CF:** The **formatcf** command formats a new CF with the Linux file system format so that Linux recognizes it.

- **getsvcstatus - Get service status:** The **getsvcstatus** command displays details about all services on the switch. Regardless of the state of a service, this command displays it. (Therefore, it also shows whether a service even exists.) The command can display a particular service or all services. A service name is case-sensitive, so it must be entered exactly. To see the spelling of a service name, use the **all** or (*) argument **getsvcstatus**. An example of **getsvcstatus all** follows this syntax line:

  Syntax: **getsvcstatus <*service name*> *** or **all**

```
>getsvcstatus all
- Services -
Name          Root  Enabled State  PID  Restarts Max        Interval   Exe

CEService     No    Yes     READY  879    0      0x0FFFFFFF   10000/shoretel/
bin/CEService

CMService     No    Yes     READY  884    0      0x0FFFFFFF   10000/shoretel/
bin/CMService

CSISVMService No    Yes     READY  889    0      0x0FFFFFFF   10000/shoretel/
bin/CSISVMService

MailServ      No    Yes     READY  930    0      0x0FFFFFFF   10000/shoretel/
bin/MailServ

PortMgr       No    Yes     READY  2311   0      0x0FFFFFFF   10000/shoretel/
bin/PortMgr

SMService     No    Yes     READY  1004   0      0x0FFFFFFF   10000/shoretel/
bin/SMService

stts          Yes   Yes     READY  1295   0      0x0FFFFFFF   10000/shoretel/
bin/stts

TMS           No    Yes     READY  1088   0      0x0FFFFFFF   10000/shoretel/
bin/TMS

- General -
Compact flash is READY
Build version is 13.20.9300.0
Server time is Mon Feb 4 19:24:15 2008
mem usage: total 516312, used 503272 (97.5%)
- Top 6 memory users -
PID    Mem% Exe
1295   6.7% /shoretel/bin/stts
930    3.3% /shoretel/bin/MailServ
1088   2.7% /shoretel/bin/TMS
2311   2.4% /shoretel/bin/PortMgr
889    1.4% /shoretel/bin/CSISVMService
884    1.2% /shoretel/bin/CMService

- Processes using more that 10% cpu -
none
- Storage -
Filesystem       1K-blocks        Used   Available  Use%  Mounted on
rootfs                51200       30000       21200   59%   /
/dev/nand/mtdblock/2  51200       30000       21200   59%   /
/dev/nand/mtdblock/1   5120        2368        2752   47%   /boot
/dev/nand/mtdblock/3 205696       44128      161568   22%   /nand
/dev/ram0            258156         112      258044    1%   /tmpfs
/dev/kcfa1           984871      296707      638119   32%   /cf
curlftpfs         7999999992           0  7999999992    0%   /ftproot
```

Figure 5-7

- **killsvc -9 - Kill service:** The **killsvc -9** command immediately kills all Linux services on a V model switch.

  Syntax: **killsvc <*service name*> *** or **all**

- **q (or Crtl-c) - Quit SVCCLI:** Entering the letter **q** or doing a **Ctrl-c** terminates the SVCCLI and returns the user to the Linux CLI.

  Syntax: **q** or **Ctrl-c**

- **reboot [idle] - Reboot (if switch is idle):** The **reboot** command causes the V model switch to reboot from NAND memory. With the optional **idle** argument, the reboot happens only if the switch is idle.

  Syntax: **reboot [idle]**

  Rebooting a V model switch and ***restarting*** a V model switch have different scopes. On other ShoreGear switches, rebooting and restarting are essentially the same. Rebooting a V model switch includes the Linux kernel and everything that a kernel reboot entails. In contrast, restarting a V model switch affects only the application layer.

- **restart [idle] - Restart services (if switch is idle):** The restart command stops and then re-starts services. The **idle** option means that the operation waits until the process is idle. For instance, restarting the stts process when idle means waiting for stts not to be handling any calls, stopping stts, and then starting it again. Also, during the course of a restart or a reboot, the switch will upgrade if necessary.

  Syntax: **restart [idle]**

- **restorevm - Restore voice mail files:** The **restorevm** command causes the backed up VM, Auto-Attendant, and logs to be restored from the server to the CF card. voice mail operation is unavailable during a restore. This process overwrites whatever is on the CF cards and puts the V model switch in the same state it was in at the time of the backup. The restore operation must be started from the SVCCLI. (The Director provides no option for starting a restore operation.) When the restoration is complete, the SVCCLI posts a message, and the switch is restarted.

- **sendcmd - Send command:** The **sendcmd** command causes Linux to send a command to a particular service. This command is used by ShoreTel engineers for debug only.

  Syntax: **sendcmd** <***service name***>

- **startgroup - Start group of services:** The **startgroup** command starts a group that has been stopped. This command is the followup to the **stopgroup** debug command.

  Syntax: **startgroup** <***group name***> * or **all**

- **startsvc - Start service:** The **startsvc** command starts one or all services that have been stopped. This command might be able to restart one or more services that have stopped working. It can also be the followup to the **stopsvc** debug command.

  Syntax: **startsvc** <***service name***> * or **all**

- **stopgroup - Stop group of services:** The **stopgroup** command stops one or all service groups. It kills the targeted group's process.

  Syntax: **stopegroup** <***group name***> * or **all**

- **stopmgr - Stop services manager:** The **stopmgr** command completely stops the operation of the services manager.

  Syntax: **stopmgr**

- **stopsvc - Stop service:** The **stopsvc** command completely stops one or all services. It kills the targeted service's process.

  Syntax: **stopsvc** <***service name***> * or **all**

5.5.3 CLI

Table 5-2 lists the CLI commands. Refer to Section 5.2.2.3 for a description of CLI.

Command	Description	Notes
adm_debug_level	Logs admission control and bandwidth manager signal flow onto serial port.	=2 logs more diagnostics.
adm_diag_level	Logs admission control and bandwidth manager signal flow into IPBX log.	=2 logs more diagnostics.
arpShow and arptabShow	Displays the ARP table.	
autoReboot = 0	Turns the switch watchdog off to prevent rebooting after a catastrophic failure.	Use this command only when directed by ShoreTel Customer Support.
bigNvRamSetup	Erases switch's configuration in NvRam.	
bootChange	Changes the boot ROM parameters.	Use with caution.
cid_debug_level	Logs caller ID related information for extensions.	
cliStart	Opens the ShoreTel command line interpreter from a serial port.	Reboot the switch to return to the Linux interface.
config_status	Outputs the configuration records for the switch.	
DEBUG_LEVEL	Sets the ShoreSIP debugging flags.	Recommend using level 0xe00.
diagdCommands	Outputs full switch diagnostic information.	
dial_num_dump	Displays information about switch's off-system extension configuration.	
dn_plan_status	Displays information about the switch's dial plan.	
dnp_debug_level	Displays detail information (digit by digit) about dial plan access.	Recommend using level 1.
dtmf_debug	Displays RFC2833 for G729 related events.	Values can be 0 or 1 (default is 0).
DumpSB	Displays maximum PMCSW outputs.	
DumpSRAM	Displays Motorola 860 processor information.	For IPBX model switches only.
dumpUsedBw	Displays information about actual bandwidth used on individual calls/legs.	
etherMonBroadcast	Writes the ethernet broadcast messages to a .cap file in \inetpub\ftproot directory of the ShoreWare server that are not intended for that switch.	Recommend using level 1.
etherMonDump	Writes the ethernet trace information captured when using EtherMonStart. Writes to a .cap file in \inetpub\ftproot directory of the ShoreWare server controlling the switch. The .cap file name is ST-<lst 3 bytes of MAC-time-date>.cap.	
etherMonStart <bytes>	Bypes is the number of bytes of information you want to capture (for example, 10000000). Captures ethernet packets for trace purposes	Command consumes switch memory. Run *memShow* to display available memory. Do not specify more than available.
etherMonStop	Stops capturing ethernet packets.	

Table 5-2 CLI Commands

Command	Description	Notes
eval_adm_var	Displays information about switch's own bandwidth usage.	
eval_bwm_var	Displays information about total and available bandwidth.	
ext_bca_status	Displays active BCA calls along with call stack usage information.	To be run on switches hosting BCA extensions.
ext_cco_status	Displays information the switch's extension CCOs.	
ext_conf_status	Displays MakeMe conference port status.	
ext_debug_level1	Logs extension CCO configuration.	
ext_debug_level	Sets the extension debugging level.	Recommend using level 4.
ext_pg_status	Displays active pickup group calls.	To be run on the switches hosting PG extensions.
fax_debug_level	Display fax-related events and processes, incluidng tone detection, fax determination, and fax redirect.	Values can be 0 or 1 Default is 0
fax_verbose	Used to display fax/silence detection, jitter buffer freezing. and echo canceller disabling related events.	Values can be 0 or 1 Default is 0
flsh_getVersion	Displays switch’s firmware and bootrom versions.	
flsh_printBootLine	Prints the boot parameters of the switch.	
flsh_setBootSourceFlash	Sets the switch to boot from flash memory.	Restart to enable changes.
flsh_setBootSourceFTP	Sets the switch to boot from FTP.	Restart to enable changes..
g729_verbose	Displays more information for G729 calls.	Enable this for G729 calls with mscmd_verbose
hostShow	Displays the known hosts.	
hunt_load_debug	Logs basic huntgroup call flow.	For debugging heavy call load issues.
icmpstatShow	Displays ICMP statistics.	
ipdt_debug_filter	Assume two extensions in the system: Ext A and Ext B. To print out IPDT log for Ext A. > ipdt_debug_level = -1 > ipdt_debug_filter=1 (tell IPDT that we enable filter) > ipdt_restrictTraceExts "Ext A's#" (turn on log for Ext A) > ipdt_remRestrictTraceExt "Ext A's #" (turn off log for Ext A). To print log for all extensions: > ipdt_debug_filter =0	
ipdt_debug_level	Recommend setting to **= -1** to turn on all loggings.	
ipdt_dumpCCOCK	Dumps BB call key state, since there is no extension associated with BB.	
ipdt_dumpExtCalls	Dumps call information in the extension (e.g. callID, legID, call state and leg state, etc.)	
ipdt_dumpExtDisplay	Dumps the current display view from IPDT.	

Table 5-2 CLI Commands

Command	Description	Notes
ipdt_dumpExtensions	Dumps information for all extensions controlled by the switch and the information for monitored extensions and MAE (BCA) extensions that are in the same switch and in the different switches.	
ipdt_dumpExtCK	Dumps information for call keys on the extension. Useful for troubleshooting LED patterns and icon issues.	
ipdt_resetExtDisplay	Redisplay on the extension. If the phone display and IPDT display (ipdt_dumpExtDisplay) are desynchronized, we can run ipdt_reset_ExtDisplay to synchronize them.	
ipdt_restrictTraceExts	Set ipdt_debug_filter to 1. Then, use ipdt_restrictTraceExts to turn on logging on a particular extension.	
ifShow	Displays the current configured network parameters.	
laa_debug_level	Logs backup auto attendant signal flow.	
lspConList	Displays switch connectivity to other switches.	
lsp_debug_level	Displays Location Service Protocol messages that are exchanged between switches.	Recommend using level 4.
lsp_ping	Tests the LSP UDP communication to the far end switch for 100 iterations. Tests LSP UDP communication to the switch at 192.168.1.1, for 100 iterations (nominally 1 second). If only the IP address is supplied, 1000 iterations (nominally 10 seconds) is used.	example -> lsp_ping "192.168.1.1",100
lspTelList	Displays local and remote contacts.	
lspTelList 1	Displays detailed information about local contacts.	
lspTelList 2	Displays detailed information about remote contacts.	
mae_debug_level	Logs BCA call flow information.	
mailbox_debug_level	Logs mailbox destination for a particular call.	
memShow	Shows current memory usage of the switch.	
mgcp_msg_debug	Logs MGCP messages.	
mgcp_trans_debug	Logs MGCP transactions.	
mohc_debug_level	Prints diagnostic information for music on hold calls when set to 1.	Valid settings are 0 and 1. Default is 0.
mpm_debug_mask=0x40	Sets mpm debug flag to output Caller ID information received on inbound calls.	
mpm_debug_mask=0x10	Displays detailed DTMF information.	
mpm_debug_mask=-1	Displays detailed mpm information. Full debug of inbound calls (CallerID, DTMF).	
mscmd_verbose	Prints diagnostic information for the media commands sent from Switch board layer when set to 1.	Main media command verbose variable. Default is 0.
msps	Displays media stream statistics for all active calls on the switch.	This is a helpful command for all media-related issues.
msps 7	Displays media stream statistics for active calls.	

Table 5-2 CLI Commands

Command	Description	Notes
msps 8	Displays media stream statistics.	Use only when directed by ShoreTel.
msps 16	Displays media stream statistics.	Use only when directed by ShoreTel.
mwi_debug_level	Logs message waiting indicator setting call flow.	
ping "<*IP Address*>"		Include double quotes (“) around the IP address.
pri_log=4	Begins output of D-Channel information.	Must be in Remote Shell on IPBX model switches. (Recommend 4)
pri_trace=4	Sets the PRI D-Channel trace debug level.	Must be in Remote Shell on IPBX model switches. (Recommend 4)
pri_verbose	Traces a high level description of the PRI traffic sent and received by trunks on the switch.	Recommend setting pri_verbose=1
print_ether_stats	Prints the Ethernet statistics from the network controller.	
rdn_diag_level	Used to determine why calls are routing to particular destinations, similar to what gets put in the DRSMain log when DRS is enabled.	Useful values are 0 (none) or 5 (trace resolve_dn).
reboot	Reboots the switch.	
Record2File2(port,time, <file_name>;0)	Records inbound media on the specified port for the specified time (in seconds) and writers it to /inetpub/ftproot.	Writes to the TMS server controlling the switch. FTP write access must be enabled on the server.
rfc2833_for_g711_debug	Displays events related to RFC2833 for G711.	Bitmask integer. Valid settings are 0, 1, and 2. Default is 0.
routeShow	Displays current routing table.	
routestatShow	Displays routing statistics.	
sb_debug_level	Switch board debug variable that prints debug information for the commands sent from Call control.	Values range from 1-5.
set_mpm_debug (char *)	Used to print information regarding commands/event interface between host CPU and DSPs.	Uses a string as a parameter (e.g. “pots”, “pstn”, “dtmfd”, “dtmfg”, “cdis”, “class”, “cpm” are valid parameters). Example: To print POTS related information, use set_mpm_debug(“pots”)
sip_debug_level=1	Logs ShoreSIP to SIP translation.	
sip_debug_level=2	Logs SIP messages also.	
sipuaCallList	Displays active SIP stack calls. sipuaCallList 2 dumps more call related information.	For switches hosting SIP trunks/extensions.
sipuaList	Displays list of SIP trunk/extension user agents.	For switches hosting SIP trunks/extensions.

Table 5-2 CLI Commands

Command	Description	Notes
t2t_debug_level	Logs trunk interval information like silence, trunk name, trunk state, etc.	
tcpstatShow	Displays TCP statistics.	
trans_debug	Logs ShoreSIP transactions.	
traceroute "<*IP Address*>"	For troubleshooting network by mapping route packets use to traverse an IP network.	Include double quotes (“) around the target IP address. Section 5.4.4 on page 78.
trunk_cco_status	Displays information about switch's trunk CCOs.	
trunk_debug_level	Sets the trunk debugging flag	Recommend using level 4.
uaCallList	Displays information about active calls and legs.	
ua_call_status	Shows a snapshot of the active call status of the switch.	
uaList	Displays list of ShoreSIP extension/trunk user agents.	
unset_mpm_debug(char*)	To disable **set_mpm_debug** command	
udpstatShow	Displays UDP statistics.	

Table 5-2 CLI Commands

5.5.4 Cfg Utility

Table 5-3 summarizes commands available through the **cfg** utility. Variables are italicized. Refer to Section 5.2.3.2 for a description of the cfg utility.

Command	Parameters	Description	Comments
call *p*	*p* = phone number	Make a call from the voice mail application and play a prompt.	
closem		Close the open voice mail box.	
dmask *0x*	*0x* = mask hex	Set voice mail debug mask (hex)	Enter without parameter sto display flag list.
exit		Leave cfg.	
laam *t*	t = (1 = DID, 2 = DNIS, 3 = Trunk)	List Auto-Attendant menu map.	Displays mapping of trunks to Auto-Attendant menus.
lall *f*	f = 1 for more details	List all mail boxes in the system.	Enter without “1” for a summary of system mail boxes and with “1” for more detail.
lamp *m f*	*m* = mail box *f* = 1 - on; 2 - off	Turns the message waiting light on/off for a specified mail box.	
list pb b	b = (0 - last name, 1 = first name)	Dump dial by names directory to the voice mail log.	
lmbox *f*	f = 1 for more details	List mail box information.	Enter without “1” for a system mailbox summary, including message IDs.
lms		List mail box schedule.	
lmsg *m*	*m* = message ID	List details of a specific message.	Message IDs can be found by using lnbox.
loadc		Load all voice mail configuration from the database.	
loadm		Load all mail box configuration from the database.	Requires that a mail box be open when you issue the command.

Table 5-3 cfg Commands

Command	Parameters	Description	Comments
lserv		List information about all servers.	
lsys		List voicemail system parameters.	
lsmtp		List status of distributed voice mail.	
ltapi		List status of TAPI lines opened by voice mail.	
msinfo		Dump voice mail internal table to the voice mail log.	
openm #	# = mail box	Open specified mail box.	
psinfo		Dump port server information to the voice mail log.	
purge		Remove message in the deleted queue.	Requires that a mail box be open when you issue the command.
sh *str*	*str* = string	Search help for a string.	Searches only from the beginning.
starth		Remove old deleted messages.	
symwi		Run MWI synchronization.	Sends MWI status to all phones in system.
ver		List cfg version.	
?		List help commands.	

Table 5-3 cfg Commands

5.5.5 UBOOT

5.5.5.1 UBOOT Commands

Table 5-4 a list of UBOOT environment variables.

Parameter	Description	Flash Boot	FTP Boot
autoload	Specifies booting method for bringing up operating system	FLASH	FTP
bootcmd	Specifies boot actions that loads OS and software onto switch.		
bootfile	Path and filename of operating system file	tskl/uImage	tskl/uImage
flags	Variable passed to Linux that controls post startup operations.	0x40	0x40
gatewayip	IP address of gateway server	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
host	IP address of host running Director	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
ipaddr	IP address of the switch	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
netmask	Subnet mask for subnet location of the switch	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
pass	Password for FTP account.	default setting is ***tsk***	default setting is ***tsk***

Table 5-4 Parameter Settings for Flash Boot and FTP Boo

Parameter	Description	Flash Boot	FTP Boot
script	Path and filename of bootscript file	tskl/bootflsh.txt	tskl/bootscrp.txt
serverip	IP address of host from which FTP transfer retrives the OS image.	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx
user	User name of FTP account.	default: ***anonymous***	default: ***anonymous***

Table 5-4 Parameter Settings for Flash Boot and FTP Boo

5.5.5.2 UBOOT Flags

The following is a list of actions triggered by flag values:

- 0x0: Auto-negotiate network speed and duplex mode
- 0x20: Disable login security
- 0x40: Use DHCP to receive boot parameters
- 0x1040: Use bootp to receive boot parameters
- 0x2000: Disable ShoreTel shell
- 0x10000: 10 MB full duplex (fixed)
- 0x20000:10 MB half duplex (fixed)
- 0x30000:100 MB full duplex (fixed)
- 0x40000:100 MB halfduplex (fixed)

Multiple functions are specified by adding the hex values of the individual functions. For example, the command 0x42040 instructs the swithch to use DHCP to receive boot parameters (0x40), disable the ShoreTel Shell (0x2000) and set the speed and duplex mode to 10 Mb, half duplex (0x40000).

5.5.6 Burnflash

The following table summarizes burnflash commands.

Command	Description
burnflash -s <*Switch IP Address*>	Updates all bootrom areas.

Table 5-5 Burnflash Commands

5.5.7 ipbxctl

The following table summarizes ***ipbxctl*** commands:

Command	Description
-reboot <*Switch IP Address*>	Reboots the switch without using ShoreWare Director.
-flash <*Switch IP Address*>	Sets switch to boot from flash memory (allows you to boot without logging in).
-ftp <*Switch IP Address*>	Sets switch to boot from FTP (allows you to do this without logging in).

Table 5-6 ipbxctl Utility Commands

Command	Description
-diag <*Switch IP Address* >	Sends switch state information. By default, the system puts this information in the same folder where ipbxctl utility is running. This may be distruptive to normal switch function. Use this command only for diagnostic functions, not for reporting.
-reset	Clears all flash memory. Returns switch to factory defaults.
-traceroute <*target IP Address* >	Network troubleshooting tool. For additional information about the parameters that can be used with this command, Table 5-1 on page 79 of this chapter.

Table 5-6 ipbxctl Utility Commands

5.5.8 regedit

5.5.8.1 regedit Commands

```
key <keyname>[\<keyname>]... - make subkey <keyname> current key
<keyname>[\<keyname>]...     - make subkey <keyname> current key
.                            - display current key, values recursively
                              depending on display mode 'd'
key .                         - display current key, values recursively
                              depending on display mode 'd'
*                             - display current values
key *                         - display current values
..                            - up one level
key ..                        - up one level
addkey <keyname>              - add subkey <keyname> to current key
delkey <keyname>              - delete subkey <keyname> from current key
addstr <valname> <strvalue>   - add <valname> <strvalue> to current key
addnum <valname> <numvalue>   - add <valname> <numvalue> to current key.
                              <numvalue> is <base10digit>...
addhex <valname> <hexvalue>   - add <valname> <hexvalue> to current key.
                              <hexvalue> is 0x<hexdigit>...
setstr <valname> <strvalue>   - set <valname> <strvalue> in current key
setnum <valname> <numvalue>   - set <valname> <numvalue> in current key.
                              <numvalue> is <base10digit>...
sethex <valname> <hexvalue>   - set <valname> <hexvalue> in current key.
                              <hexvalue> is 0x<hexdigit>...
delval <valname>              - delete value <valname> from current key
d                             - toggle recursive display
q                             - quit program
< filename                    - To read commands from a file
   E.g RegEdit < cmdfile
   Where cmdfile has the following contents
   VoiceMail
   Logging
   sethex Level 0xff
```

5.5.8.2 Registry Keys

The ShoreTel software utilizes the Windows registry to store various parameters used by the ShoreTel system. These registry keys can be found in the following registry path:

- Switch Software Registry Keys
  - allow_cfa_deactivation
  - auto_onhook_for_handsfree

- auto_onhook_for_hold
- busy_all_huntgroups
- disable_oae_over_sip
- display_hunt_group_on_phone
- fastblink_held_bca_call
- give_bca_reminder_ring
- onhook_dialing_for_IP110
- rtcp_enabled
- send_3_1_khz_audio
- send_bca_cid
- send_ecma_rose_qsig
- send_isdn_setup_sending_complete
- sorted_trunks
- timeout_icmp_redirect
- timeout_overhead_paging

- Telephony Management Server (TMS) Registry Keys
  - CDRDataExpiration
  - CDRDataCacheSize
  - LogAssertsAsNTEvents
  - SwitchDebug

- Voice Mail Registry Keys
  - AutoDelete_Override
  - AutoDelete_ExpHrs
  - AutoDelete_Warn1Hrs
  - MWIDelay
  - RecallMessageEnabled
  - TimeOutWaitConnect
  - PlayShorelineFwdCallMsg
  - PlayLogonFindMeBranding
  - PlayHeardMessagesLIFO
  - AttachNoVMToEmail
  - LangLoad_Override
  - Allow_SMDI_VM_ChangeCHM
  - SMDI_FlashDuration
  - SMDI_WaitForDialTone
  - SMDI_DelayBeforeSendingDigits
  - SMDI_DelayBeforeHangUp
  - SMDI_SendName
  - SMDI_FillCharacter
  - SMDI_SendMWIError
  - FromID
  - SMTPRoutesFile
  - MaxMessageSizeFile
  - SMTPClientConnTimeoutFile
  - SMTPClientDataTimeoutFile
  - SMTPServerDataTimeoutFile
  - MaxConcurrentIncomingFile
  - MaxConcurrentRemoteFile

5.5.9 ShoreWare File System

5.5.9.1 Server Files

The following list identifies the directories where the ShoreWare server installs its files.

The server installs files with default access permissions. (System administrators may want to ensure a more secure environment.)

The Windows System user and the IPBX user created by the ShoreTel installer require full access to all the ShoreWare directories. All other users can be granted access on an as-needed basis.

To ensure the security of sensitive and/or personal information, confine access to the VMS and Database directories strictly to administrator, system, and IPBX users.

- **Shoreline Data:** Contains all the dynamic information the server uses to run the system. This directory and all sub-directories may be saved as part of a backup and used for full system recovery. <drive>\Shoreline Data
- **Prompts:** Contains copies of the menu prompts.
  <*drive*>\Shoreline Data\Prompts
- **VMS:** Contains all the files and configuration information used by the voice mail system. The files in this directory and its sub-directories are very dynamic and should never be opened. Opening any of the configuration files may cause the voice mail system to become corrupted in part or completely, and can cause loss of voice mail messages.
  <*drive*>\Shoreline Data\VMS
- **MESSAGE:** Contains all voice mail messages as .wav files, along with an .enl pointer file for each message.
  <*drive*>\Shoreline Data\VMS\MESSAGE

5.5.9.2 Compact Flash Files

V model switches use the Ext3 file system on the CF card. (Therefore, with software on a PC that can read Ext3 files, the user can plug the CF card into a PC and access the voicemail.)

CHAPTER 6

IP Endpoints

6.1 Overview

The ShoreTel system manages calls and applications for three types of IP endpoints: IP phones, SoftPhones, and conference bridges. IP endpoints are identified by IP address and can exist anywhere on the network. All IP endpoints are supported by ShoreGear switches, which must have sufficient capacity for all the IP endpoints in the system. IP endpoints are configured in the system with ShoreWare Director. For more information on IP endpoints, see your ***ShoreTel 8 Planning and Installation Guide*** and ***ShoreTel 8 Administration Guide***.

6.1.1 IP Phones

ShoreTel IP phones allow you to deploy your telephony system as an end-to-end IP network without dedicated station wiring. Connecting anywhere on the network, ShoreTel IP phones work with the ShoreTel Call Manager client applications or can be used independently, providing an intuitive interface to essential telephone features.

The IP phone controls basic display operations, such as volume level, date and time, and icons. To provide IP telephony in a ShoreTel system, IP phones rely on services, switches, and industry-standard protocols. The following sections describe these dependencies.

ShoreTel IP Phones

- ShorePhone-IP100
- ShorePhone-IP110
- ShorePhone-IP115
- ShorePhone-IP210
- ShorePhone-IP212k
- ShorePhone-IP230
- ShorePhone-IP230g
- ShorePhone-IP265
- ShorePhone-IP530/560/560g
- ShorePhone-IP565g

6.1.1.1 IP Phone Keep Alive

The ShoreGear-120/24, ShoreGear-60/12, and ShoreGear-40/8 voice switches send a heartbeat to their associated IP phones once a minute. If the heartbeat is not acknowledged within approximately four seconds, the switch considers the IP phone to be offline or unavailable. The switch continues to broadcast the heartbeat every minute. Any currently offline IP phone that returns an acknowledgement is considered online and available.

6.1.1.2 IP Phone Failover

IP phones can be optionally configured to send a heartbeat to their ShoreGear switch every four minutes. If an IP phone cannot communicate with its switch, the phone automatically connects to another switch located at the same site. For IP phone failover to be effective, the system must be planned with sufficient excess capacity to handle phones from at least one switch during a failover event. For example, if a switch with 20 IP phone ports fails, 20 IP phone ports need to be available elsewhere in the system. For more information, refer to the IP phone configuration settings in the ***ShoreTel 8 Administration Guide***.

6.1.1.3 Services

There are two services running on the ShoreWare server that interact with the system's IP phones: IP Phone Configuration Service (IPCS) and IP Phone Display Service (IPDS).

IPCS

The IP Phone Configuration Service manages the IP phone configuration process, including configuration files and the database updates. Problems with IPCS connectivity can prevent IP phones from booting and prevent phone configuration data from being updated.

IPDS

The IP Phone Display Service handles the remaining functions, such as event handling and feature button functions. It also controls any actions by the IP phone display not controlled by the device's firmware or switches. Problems with IPDS or TMS connectivity can result in incorrect phone displays and errors in both the hard and soft key functions.

Embedded IP Phone Display Driver

These features will not be handled by the switch but will continue to be provided by the server. Control of many of the IP phone features (such as phone display, redial, and call transfers) has been shifted from the server to the switch in order to enhance reliability and offer better uptime. Features that require writing to the database (such as directory and speed dial) will continue to depend on the server being both operational and accessible.

Date and Time

IP phones depend on an SNTP server to maintain the correct time and date. Without an SNTP server, you can set the phone date and time via a GMT offset. For more information, see Section 6.6.3 on page 125.

6.1.1.4 IP Phones and ShoreGear Switches

IP phones in a ShoreTel system interact with two types of ShoreGear switches: the configuration switch and the call manager switch. The configuration switches help the IP phones obtain their configuration from the ShoreWare server, which functions as a FTP server for the IP phones. You must have at least one configuration switch and can designate a second configuration switch for reliability.

As part of the configuration information, each IP phone is assigned a ShoreGear switch that acts as the phone's call manager to help the IP phone set up and tear down calls.

Configuration Switch(es)

In a DHCP environment, when an IP phone is booted, it receives the IP address of the DHCP and ShoreWare server from the configuration switch. Each system has at least one configuration switch for this purpose. The IP addresses of these switches are downloaded to the IP phones whenever the IP phones are booted.

If you have configured the IP phones to boot without a DHCP server, you must set the IP address of the configuration switch manually. For more information, see Section 6.6.3 on page 125.

These switches communicate with the ShoreTel server to determine which switch manages calls for a particular IP phone. You have the option of assigning two switches to this function, in case one fails. For information on configuration switches, see the ***ShoreTel 8 Administration Guide***.

Call Manager Switch

The IP phones' ShoreGear switch is responsible for actions such hold, transfer, conference, and park. The call manager module of the ShoreGear switches handles the Media Gateway Control Protocol (MGCP) information from the IP phones assigned to it. Once a call has been connected to an endpoint, media streams are independent of the call manager switch.

The ShoreGear switch communicates call information to other switches in the system using ShoreTel's enhanced SIP protocol. Every site where IP phones are in use must have a ShoreGear voice switch configured to support the number of IP phones at the site.

The ShoreGear voice switches send a heartbeat to the IP phones once a minute. If the heartbeat is not acknowledged within approximately four seconds, the switch considers the IP phone to be offline or unavailable. The voice switches continue to broadcast the heartbeat every minute. Any currently offline IP phone that returns an acknowledgement is considered online and available.

To configure IP phone support on a ShoreGear-120/24, ShoreGear-60/12, or ShoreGear-40/8 voice switch, you must reserve ports for IP phone support on the ShoreGear Switch edit page in ShoreWare Director. See the "Configuring Switches" chapter in the ***ShoreTel 8 Administration Guide*** for additional information.

6.1.1.5 IP Phone Communications

MGCP

IP phones communicate with ShoreGear switches via MGCP, a device control protocol. The relationship between the switch (call manager) and the phone (gateway) follows a master–slave model.

MGCP, an industry-standard protocol, is used to:

- Deliver information to the IP phone display
- Set up and tear down media streams
- Report phone events such as key presses, on hook, and off hook

Media

Media travels through the ShoreTel system using Real-Time Protocol (RTP). After call setup, media flows directly between IP phones via RTP. The ShoreGear switch is involved only when setting up or tearing down a call.

For more information on MGCP and RTP communications, see Section 2.3 on page 7.

6.1.2 Boot Process

ShoreTel IP phones are preconfigured by ShoreTel to work in conjunction with your ShoreTel system and your network's Dynamic Host Configuration Protocol (DHCP) server. Once the servers are configured, you simply plug the phones into the network and they are automatically added to your ShoreTel system.

Once the IP phone has the DHCP and FTP server IP addresses, it downloads the application and configuration files from the FTP server. The IP phone configuration file is modified by ShoreWare Director during IP phone configuration.

If you are not using a DHCP server or it is not currently online, you can set a static IP address and other startup parameters directly at the IP phone. Static IP addresses for IP phones can also be assigned using the IP phone setup menus. For more information, see Section 6.6.3 on page 125.

6.2 Maintenance

6.2.1 IP Phone Firmware Upgrades

The IP phone application software can be upgraded by replacing the application file on the FTP server. If you need to upgrade your phone application, refer to the instructions provided with the new phone software.

WARNING Modifying the IP phone configuration files can cause unpredictable results. If you have special needs, contact ShoreTel Customer Support for instructions.

6.3 Diagnostics

The following recommendations will help you install your IP phones:

- Make sure you have reviewed your network bandwidth and Quality of Service (QoS) strategies and configured your network for your IP phones.
- Make sure the phones are configured to use DHCP vendor option 155 for configuring boot server information, and are configured to use anonymous FTP.

  The phones will not boot properly if static configuration data is present in the telephone. This can occur if the telephones were previously used in an environment where DHCP and automatic provisioning was not used, or the telephone is from a vendor other than ShoreTel. See Section 6.6.3 on page 125 and Section 6.4 on page 107 for information about changing the telephone to the correct settings.

6.3.1 Viewing System IP Phones

IP phone connectivity can be viewed from the **IP Phone List** in ShoreWare Director. The ShoreGear-120/24, ShoreGear-60/12, and ShoreGear-40/8 **Switch Maintenance** screens have an additional section for IP phone maintenance. This shows how many IP phones are connected through the switch and the capacity of the switch. ShoreGear-24 switches can support as many as 120 IP phones, the ShoreGear-60/12 can support up to 60, and the ShoreGear-40/8 can support up to 40 IP phones. For more information, see the ***ShoreTel 8 Administration Guide***.

6.3.2 Onscreen Error Messages

Any time a user action results in an error being returned by TAPI, the error is displayed on the IP phone display for six seconds (one North American ring cycle). The error message can be dismissed sooner by pressing the "OK" soft key.

6.3.3 Diagnostic and Failure Messages

The table below outlines the diagnostic and failure messages that may be displayed on ShoreTel IP phones.

Display Message	Interpretation
File System Failure	An internal, unspecified, problem has been detected while performing a file system operation.
Boot File Too Big	The boot file is too big and won't fit in RAM
Boot Save Failed	Writing the boot image to flash memory failed.
Reconfiguring Network	The phone is switching VLANs. This might be displayed after DHCP and/or after config file processing.
Duplicate IP Address	Arp of IP address indicated the IP address we are attempting to use is already in use.
FTP Unreachable	The FTP server could not be pinged (for IP110)
FTP Server Unreachable	The FTP server could not be pinged (for others)
Unresponsive task/Resetting…..	A task failed to respond to a keep alive request so the phone is restarted
DSP Error/Repair Required	DSP testing failed on startup. Bad DSP.
NO MGC IP CONFIGURED	An IP address has not been set for the MGC
DSP Asserted/Resetting…	The DSP has crashed and we will be rebooting.
DHCP lease/invalid!	The DHCP lease expired and the phone failed to acquire a new lease.
APP download failed!/filename	Application image download failed
Invalid App Name	The application name does not follow the required format
Format Failed	While trying to store a new image in flash, a failure occurred when erasing the flash device.
File System Error	An error was returned by the file system API.
Invalid Signature	The boot or application image file is the wrong type for this phone
Invalid Image Version	The .bmp image was not of a known acceptable format
Download CFG file failed/filename	Failed to download the main configuration file specified.
Couldn't Get INCL file/filename	Failed to read the specified Include file from the FTP server
Using Cached CFG (for IP110) Using Cached CFG Files! (for others)	If a complete config file and all includes cannot be downloaded a cached config file is being used.
Enter Factory mode/*=No #=Yes	In Response to mute-rramos
Factory Test KPD Mode	You are in factory test mode ready to test the keypad (via mute-rramos)
Example Application	This message is a remnant of some test code and should never be seen.
Boot Application	If only a boot application is in flash and an application image cannot be downloaded, this will be displayed after the boot process completes.
No/Ethernet	Ethernet is not detected
100 Mbps/Ethernet	100 Mbps Ethernet speed in use

Table 6-1 Diagnostic and Failure Messages

Display Message	Interpretation
10 Mbps/Ethernet	10 Mbps Ethernet speed in use
Request Service (for IP110) Requesting Service (for others)	Being requesting service from MGC
No Service	MGC service is unavailable

Table 6-1 Diagnostic and Failure Messages

6.3.4 IP100 Phone Troubleshooting

If an IP100 phone becomes unresponsive or behaves in an undesired fashion, use the following diagnostic steps to collect diagnostic information and forward to ShoreTel Customer Support for analysis.

Step 1 Record the IP address and MAC address of the problematic IP phone. These can be found in Shoreware Director under **IP Phones** and **Individual IP Phones**.

Step 2 On the IP phone, press the menu button and record any information displayed on the screen.

Step 3 Record the state of the IP phone. View the IP phone state by selecting the IP phone's host switch in QuickLook and clicking **IP Phones Maintenance**. Record the IP address of the host switch.

Step 4 Ping the problematic IP phone using the 'ping' command on the IP Phones Maintenance page.

`Ping xxx.xxx.xxx.xxx` (IP address).

If the IP phone returns the following message(s), go to Step 5.

```
Reply from xxx.xxx.xxx.xxx: bytes=32 time<10ms TTL=64
```

Step 5 If you do not receive a response to the ping command, collect application and boot logs in the *inetpub\ftproot* directory, stop here, and send the available information to ShoreTel Customer Support. File naming convention is `IP_Phone_MAC-app.log` and `IP_Phone_MAC-boot.log`.

Example: `0004F2003896-app.log`

Step 6 On the ShoreWare server, enable a Telnet session to the host switch as follows:

Step a Open a CMD window and navigate to the *Program Files\Shoreline Communications\Shoreware Server* directory.

Step b Type `ipbxctl -telneton xxx.xxx.xxx.xxx` using the IP address of the host switch and press ENTER.

Telnet into the host switch using the `telnet` command. Use the following login name and password:

Login: `anonymous`
Password: `ShoreTel` (case sensitive)

Step c Type `ext_cco_status` and press ENTER. Capture the returned information.

Step d Type `mgcp_msg_debug=1` and press ENTER to turn on MGCP message trace.

Step e Type `ext_iphone_status` and press ENTER. Wait for 5 seconds and capture the returned information. Wait an additional 30 seconds and capture any additional output from the switch.

Step f Type `mgcp_msg_debug=0` to turn off MGCP trace.

Step 7 Restart the IP phone by either unplugging the data cable and reconnecting, or holding down the volume keys, the hold button, and the second soft key directly above the hold button for 5 seconds to initiate a restart of the phone.

Step 8 After the phone completes rebooting, collect the new application and boot logs created for the IP phone (as described above).

Step 9 Forward all the information you recorded to ShoreTel Customer Support for analysis.

6.3.5 Troubleshooting the IP Phone Display

This section presents some techniques for troubleshooting the IP Phone Display Server. The first step is to identify that the problem is actually an IPDS problem.

You should suspect an IPDS problem whenever a phone configured in the database (which appears on the IP phone list in ShoreWare Director) does not have the correct display, or doesn't respond properly when you press the feature buttons. When you suspect an IPDS problem, verify that the server has TAPI access to the phone or phones in question. To check TAPI access, use any TAPI application that supports phone devices such as TapiTest and PhoneMon.

6.3.5.1 Phone Display is Incorrect

If a phone display is incorrect, one of two things may have happened:

IPDS Sent a Bad Display Update

This can be detected by searching through the IPDS log file for the display line in question. If it is found at the appropriate time and on the appropriate extension, IPDS is the cause of the problem. Provide the relevant IPDS log to your engineering resources.

Switch Did Not Update the IP Phone Correctly

It is possible for the switch to mishandle phone updates.

6.3.5.2 Administrative Messages

The system administrator may send messages to a single IP phone or to all of them. These messages can alert users of upgrades or downtimes, or simply test the communication channel from IPDS through TMS and the switch to the phones. For details on how to send administrative messages using IPPhoneCfgTool.exe, see Section 3.3.7 on page 39.

Enabling IPDT Debugging

By default, IPDT logging is turned off. However, you can enable IPDT logging to assist in troubleshooting efforts.

6.3.5.3 Enabling IPDT Debugging

To enable logging on the switch, follow the procedure below:

Step 1 Telnet into the switch.

Step 2 Type the following command.

ipdt_debug_level = -1

Step 3 Logging output appears on the screen. You can use a software application, such as TeraTerm to capture the output and save it in a text file.

Details:

- IPDT logging should be enabled for short periods of time because the feature generates large amounts of data that consumes CPU cycles on the switch and slow it down.
- You can disable the logging feature by replacing -1 with a 0 in the command above.
- The -1 variable enables tracing for all IPDT-related components. You can selectively enable individual IPDT components by using the commands and variables listed in the table below.

Debug flag	Decimal value	Hexadecimal value	Purpose
DEBUG_HOTDIAL	2	0x2	timeouts and logic associated with hot dial / fast transfer feature
DEBUG_NCC_RAW_EVENTS	256	0x100	raw device status, call control, and IPDS helper events from switch core
DEBUG_NCC_DEVICE_INVENTORY	512	0x200	cco acquisitions and releases
DEBUG_NCC_FLOW1	4096	0x1000	ncc event handling
DEBUG_NCC_FLOW2	8192	0x2000	verbose ncc event handling
DEBUG_CONFIG_NOTIFICATIONS	65536	0x10000	configuration data and changes
DEBUG_NCC_DISPLAY_BASIC	16777216	0x01000000	logic associated with determining which "screen" is shown
DEBUG_NCC_DISPLAY_DETAILS	33554432	0x02000000	the actual display commands sent to the phones

Table 6-2 IPDT Debugging Flags

The following functions can be executed from a terminal session. String arguments must be passed in quotes. Integer arguments may be passed in decimal form, or in hex form by prefixing with 0x.

Function	Argument name	Argument Type	Purpose
ipdt_dumpExtensions	none	none	Lists all phones and extensions configured on switch, along with CCOID, and phone type where appropriate.
ipdt_dumpExtDisplay	extension number	string	shows current value of all display elements: announcement area, soft keys, custom key labels, custom key icons/leds, message waiting indicator, location and format of date and time, location of borders
ipdt_dumpCCODisplay	CCOID	integer	same as above, using CCOID as key. Use ipdt_dumpExtensions to find CCOIDs of non-extension devices such as anonymous phones.

Table 6-3 IPDT Functions

Function	Argument name	Argument Type	Purpose
ipdt_dumpExtCalls	extension number	string	lists all calls on the given extension. Works for "foreign extensions" too - that is, extensions whose call info is supplied by IPDS
ipdt_dumpCCOCalls	CCOID	integer	same as above, using CCOID as key; native extensions only.
ipdt_dumpExtCfg	extension number	string	lists configuration and extension status for extension. For foreign extensions, lists those details supplied by IPDS
ipdt_dumpCCOCfg	CCOID	integer	same as above, using CCOID as key; native extensions only.
ipdt_dumpActiveTimer	none	none	lists currently active timed objects in IPDT
ipdt_resetExtDisplay	extension number	string	redraws the entire display of the phone, by the given extension
ipdt_resetCCODisplay	CCOID	integer	redraws the entire display of the phone, by the given CCOID
ipdt_adminMsgExt	extension number	string	displays an administrative message in announcement area of given phone for ipdt_admin_timeout seconds. "" or "all" indicates all phones on switch.
ipdt_adminMsgCCO	CCOID	integer	displays an administrative message in announcement area of given phone for ipdt_admin_timeout seconds. 0 indicates all phones on switch

Table 6-3 IPDT Functions

6.3.6 Manually Configuring the Phones

If you are not using a DHCP server to provide the IP address and configuration parameters to the phone, you need to manually set configuration parameters on the phone.

You can enter the phone configuration menu at bootup or by entering a key sequence from the phone's keypad.

To manually configure the IP110/115/212k/230/530/560/560g at bootup:

Step 1 Connect the Ethernet cable into the data jack on the back of the IP phone.

Step 2 At the Password prompt, enter the default password 1234, or the password provided by your system administrator, followed by the # key.

You have four seconds to enter the password, after which the phone enters normal operation with its current settings.

The default password can be changed in ShoreWare Director. For more information, see the *ShoreTel Administration Guide*.

Step 3 Enter the values listed below when prompted. Press # to advance to the next settings or * to exit.

The phone downloads the latest bootROM and firmware from the ShoreTel server and in the process, reboots several times. When the phone displays the date and time, the boot and upgrade process is complete.

Prompt	Value
Clear all values?	Press #. (No.)
DHCP=ON	Press * and #.
IP=	Enter the IP address for the phone. Press #.
Subnet=	Enter the subnet mask. Press #.
Gateway=	Enter the gateway IP address. Press #.
FTP=	Enter the IP address of your ShoreWare server. Press #.
MGC=	Press #. (The phone will obtain the address from configuration files on the ShoreWare server.)
SNTP=	Enter the IP address of your time server. Press #.
802.1Q Tagging=OFF	Press #. Consult your network administrator before changing this value.
VLAN ID=	Press #.
Save all changes	Press #. (Yes.)

Table 6-4 Boot up configuration prompts

To manually configure an operational IP110/115/212k/230/530/560/560g from the keypad:

Step 1 With the phone on hook, press the MUTE key followed by 73887# (SETUP#).

Step 2 At the Password prompt, enter 1234, or the password provided by your system administrator, followed by the # key.

The default password can be changed in ShoreWare Director. For more information, see the *ShoreTel Administration Guide*.

Step 3 Enter the values listed in Table 5-4 when prompted. Press # to advance to the next settings or * to exit.

The phone downloads the latest bootROM and firmware from the ShoreTel server and in the process, reboots several times. When the phone displays the date and time, the boot and upgrade process is complete.

6.3.7 Displaying IP110/115/212k/230/530/560/560g Settings

You can display the phone's current IP parameters setting by entering a key sequence from the phone's keypad.

To display the phone's IP parameter settings:

Step 1 With the phone on hook, press the MUTE key followed by 4636# (INFO#). The phone will display the first two parameters.

Step 2 Press * to advance the display or # to exit. The phone will resume normal operation after the last parameter has been displayed.

6.3.8 Resetting the IP110/115/212k/230/530/560/560g

To reset the phone:

Step 1 With the phone on hook, press the MUTE key followed by 73738# (RESET#). The phone will reboot.

6.4 Diagnostics & Config for IP110/115/212k/230/530/560/560g

6.4.1 Boot Configuration Operation

Upon booting, IP phones use the FTP server address to acquire their configuration specifications. The FTP server address is determined from DHCP site-specific options (default option 156). If DHCP is disabled the FTP server address can be manually entered on the phone, and the information will be stored in the flash memory of the phone. Alternatively, if DHCP is used (but no site-specific option is returned), the FTP server returned by option 66 is used.

If the FTP server cannot be reached, or if a configuration file cannot be located, the phone uses the last successfully-loaded configuration parameters. After a phone has finished reading configuration files, the current parameters are saved into flash memory.

6.4.2 IP Phone Configuration Files

The following IP phone models are configured with text-based configuration files: IP110/115/212k/230/530/560/560g and BB24.

When an IP phone boots, it contacts the configured FTP server and reads an initial configuration file from FTP root. (This file corresponds to its coded model name.) Each of these initial configuration files, in turn, references a custom configuration file that can be manually edited by a system administrator. As phone software is upgraded, the contents of configuration files are overwritten at the time of update by `Kadotautil`, but custom configuration files are preserved across upgrades.

Configuration parameters are prioritized by the phone in the order that they are processed. Custom configuration files are the last file read. Any parameters in a custom configuration file will override previous configuration parameters. This also includes local parameters, as they are processed first, before any configuration files are read.

Parameters and values are case sensitive. A parameter and its value are separated by one or more spaces or tabs. Each parameter must begin on a new line of the text file.

Phone configuration file names are listed in Table 6-5.

ShorePhone Name	Name on Top of Phone	Model Name on Barcode Label Underside of Phone	Base Configuration Name	Custom File Name
IP 110	ShoreTel 110	S0	shore_s0.txt	s0custom.txt
IP 115	ShoreTel 115	S01	shore_s01.txt	s01custom.txt
IP 210	ShoreTel 210	S1	shore_s1.txt	s1custom.txt
IP 210A	ShoreTel 210	S1A	shore_s1a.txt	s1custom.txt
IP 212k	ShoreTel 212k	S12	shore_s12.txt	s12custom.txt

Table 6-5 Phone models

ShorePhone Name	Name on Top of Phone	Model Name on Barcode Label Underside of Phone	Base Configuration Name	Custom File Name
IP 230	ShoreTel 230	SEV	shore_sev.txt	sevcustom.txt
IP 265	ShoreTel 265	S36	shore_s36.txt	s36custom.txt
IP 530	ShoreTel 530	S2	shore_s2.txt	s2custom.txt
IP 560	ShoreTel 560	S6	shore_s6.txt	s6custom.txt
IP 560g	ShoreTel 560g	S6G	shore_s6g.txt	s6gcustom.txt
IP 565g	ShoreTel 565g	S6C	shore_s6c.txt	s6ccustom.txt
BB24	ShoreTel 24	SBB	shore_sbb.txt	sbbcustom.txt

Table 6-5 Phone models

While booting, IP phones look in FTP root for a unique configuration file "MAC.txt" (where MAC is the phone's MAC address). **Keep in mind that MAC config files should always be named in lower case. While Windows is usually not case-sensitive, the LIST command within the Windows FTP server DOES care about case.**

If MAC.txt is found, it is used to provide configuration files and configuration parameters for the phone. If MAX.txt is not found, then the phone uses the "coded-model-name.txt" file for configuration.

The format of a configuration file is:

Parameter1 Value

Parameter2 Value

Where the parameter and value are separated by one or more spaces or tabs and each parameter is on a new line of the text file (CR/LF is the nominal new line indicator).

The maximum permitted size of any configuration file is 5000 bytes.

Comments may be embedded in a configuration file by starting the line for the comment with a "#".

Additional configuration files may be included in the file by using the parameter Include where its value is the name of the file (and optionally a path) to include. All include parameters should be located in the original file downloaded from the FTP server. Includes must be located at the end of the main configuration file. The maximum number of included files is 5.

The most commonly customized configuration parameters are audio levels, discussed immediately below. Following the audio level parameters is a section of all the remaining phone configuration parameters.

6.4.2.1 Configuring Audio Levels

There are four sets of audio levels that can be custom configured: headset, handset, ringer, and speaker. Below are the default values for each type, except the 560G:

HandsetLevels: 5157,183,258,365,516,728,1029,1631,2303,3254,4596,517,13,13

HeadsetLevels: 6144,183,258,365,516,728,1029,1631,2303,3254,4596,917,13,13

RingerLevels: 130,258,410,649,1029,1631,2584,4096,6492,10289

SpeakerLevels: 8192,258,410,649,1029,1631,2584,4096,6492,10289,16306,17,17

The 560G phone's default levels are:

HandsetLevels: 4096,183,258,365,516,728,1029,1631,2303,3254,4596,344,13,13

HeadsetLevels (applies to phones using release 3.0.0):
5157,183,258,365,516,728,1029,1631,2303,3254,4596,430,13,13

HeadsetLevels (applies to phones using release 3.0.1):
5157,92,129,183,258,364,515,816,1152,1627,2298,430,13,13

To check which release your phone is using, press the **Mute** button while the phone is on-hook. Then, dial **I-N-F-O** on the keypad and press **#**. Continue pressing # to scroll through the information until you arrive at the Application File Name. If the name is *s6gap_03_00_**00**.ebin*, then your phone is using release 3.0.0. If the name is *s6gap_03_00_**01**.ebin*, then your phone is using release 3.0.1.

RingerLevels: 205,290,410,579,817,1154,1631,2303,3254,4596

SpeakerLevels: 8192,258,410,649,1029,1631,2584,4096,6492,10289, 16306,17,17

6.4.2.2 Parameter definitions

HandsetLevels
TxGain,RxGain1,RxGain2,RxGain3,RxGain4,RxGain5,RxGain6,RxGain7,RxGain8,RxGain9,RxGain10,SideTone,Handset DTMF Attenuation,Call Progress Tone Attenuation

HeadsetLevels
TxGain,RxGain1,RxGain2,RxGain3,RxGain4,RxGain5,RxGain6,RxGain7,RxGain8,RxGain9,RxGain10,SideTone,Headset DTMF Attenuation,Call Progress Tone Attenuation

RingerLevels

RxGain1,RxGain2,RxGain3,RxGain4,RxGain5,RxGain6,RxGain7,RxGain8,RxGain9, RxGain10

SpeakerLevels
TxGain,RxGain1,RxGain2,RxGain3,RxGain4,RxGain5,RxGain6,RxGain7,RxGain8, RxGain9,RxGain10,SideTone,Speaker DTMF Attenuation,Call Progress Tone Attenuation

The "TxGain" parameter sets the level of the audio transmitted from the phone onto the network. The "RxGain" values correspond to each of the 10 volume setting levels shown when one adjusts the volume on the phone. "SideTone" is the audio picked up from the microphone and transmitted to the speaker (speakerphone, handset or headset speaker) that provides feedback to the user that the phone is working.

Customer experience has shown that sometimes the RxGains are not high enough and need to be customized for an individual system. SideTone gain is very subjective, and is sometimes lowered and sometimes raised. DTMF Attenuation sets the receive DTMF level that the phone user will hear. Finally, Call Progress Tone Attenuation sets the level for the various tones played after a call is placed and before audio is connected.

The Plantronics CS50 wireless headset provides its own side tone, plus inserts 20 ms delay between the headset and the phone, which causes some people to say they hear echo when using the Plantronics headset, and in this case headset side tone may need to be reduced. When you speak, Plantronics does reduce the gain on the speaker by -24dB, but when you stop speaking, the gain is turned up, and you can hear the last little bit echoed in your ear.

For example, inserting the following line in "s2custom.txt" or "s6custom.txt" and rebooting the phone increases the headset volume settings 11 dB at the highest setting, which may be required in noisy environments:

HeadsetLevels
6144,183,258,409,649,1028,1630,2899,6491,10288,14333,917,13,13

Inserting the following line reduces the headset side tone by 6 dB, which some CS50 users prefer:

HeadsetLevels: 6144,183,258,365,516,728,1029,1631,2303,3254,4596,459,13,13

Minimum gain values are 0 and maximum are 32536. Setting values very high may saturate the speaker and create poor sound quality.

You can change gains on an individual phone by changing the configuration files and then rebooting that phone. But eventually all phones on the system will obtain these values when they reboot. We do not currently have the ability to individually configure ShoreTel IP phones.

Displaying Gain Levels

The **prtleveltabs** command can be used from telnet to display the gain levels for a device. For example, running this command on an IP 230 phone yielded the following output:

Ringer volume: 130,258,410,649,1029,1631,2584,4096,6492,10289

Speaker volume: 258,410,649,1029,1631,2584,4096,6492,10289,16306

Handset volume: 183,258,365,516,728,1029,1631,2303,3254,4596

Headset volume: 183,258,365,516,728,1029,1631,2303,3254,4596

The printed values represent the settings in the phone for RxGain1 to RxGain 10 for each device.

6.4.3 Other Customizable Parameters

In addition to changing the audio paraments, the custom configuration text files allow you to customize other parameters, such as day of week abbreviations used in time displays, use (on/off) of port 5004 for RTP traffic, and more.

WARNING The tables in the following section contain detailed information that can be used to modify the behavior and functionality of your ShoreTel system. Make sure you know what you are doing before attempting to utilize this information to modify your system. ShoreTel will not be held liable for any damage or expenses incurred through mis-use of this information. If you have any questions, please contact ShoreTel technical support services **before** you attempt to modify your system.

The phones support the following parameters. IP addresses from the keypad must be provided in dotted-decimal format. Cases are preserved in character strings unless otherwise indicated. Parameter checking is performed on all parameters to look for illegal values. Illegal values are ignored. White space within a parameter is ignored.

The file names used for AppName, BootName, and FontPixmap, IconPixmap, WallpaperPixmap and in Include parameters may also include a path to the file. Upper and lower case characters are ignored except when specified in the path or file name for these parameters to preserve operation with case-sensitive FTP servers.

For the purpose of comparing the file in flash and the value on the server only the file name and date are used. These abbreviations are used to identify the source of each parameter in the “Sources” column of the table:

Source	Abbreviation in Table
DHCP ACK	DHCP
DHCP Site Specific Option	SSON

Table 6-6 Source File Abbreviations

Source	Abbreviation in Table
Configuration File	CFG
Manual Entry Using SETUP	MAN
MGCP Message	MGCP

Table 6-6 Source File Abbreviations

Parameter	Value Type	Value	Source	Default
5004Enable	Up to 1 ASCII character	This enables or disables the special Shoretel use of port 5004 for RTP traffic. 0=Disable 1=Enable	CFG, MGCP	1
AppName	Up to 32 alphanumeric characters	This is the name of the application image that is in the telephone. The application file name can be at most 24 characters long. The combination of filename and path can be up to 32 characters long. A new application name is specified in a configuration file and is checked against the NV value to decide if a new version needs to be downloaded. The NV value is updated after a successful download and flash programming sequence.	CFG	Value from factory in NV Storage
BackLight	Up to 4 ASCII characters	Number of minutes the backlight remains on at full brightness when the phone is idle. Also, Backlight NN, where NN is a number 0-60. 0= n/a. 1-60 = number of minutes after which display is shut off	CFG	5
BackLightDim	Up to 4 ASCII characters	Number of additional minutes the backlight remains on at a DIM level after the BackLight interval has passed since an idle state was entered. Only applicable to the S6C and S36. A value of 0 will cause the backlight to remain at the dim level indefinitely.	CFG	120
BootName	Up to 32 alphanumeric characters	This is the name of the boot image that is in the telephone. The boot file name can be at most 24 characters long. The combination of filename and path can be up to 32 characters long. A new boot name is specified in a configuration file and is checked against the NV value to decide if a new version needs to be downloaded. The NV value is updated after a successful download and flash programming sequence.	CFG	Value from factory in NV Storage
Country	Up to 3 ASCII Characters	This parameter specifies the Country that is used by the Include parameter to identify a particular file to include. May be between 1 and 255.	SSON, CFG, MAN	1
DaysOfWeek	Up to 64 ASCII Characters	Comma separated list of the day of week abbreviations used by the IP210 phone to display the time. First day is Sunday.	CFG	Sun,Mon,Tue,Wed ,Thu,Fri,Sat
DHCP	1 ASCII Characters	DHCP enable/disable 0=Disabled 1=Enabled	MAN	1

Table 6-7 Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
DscpAudio	Up to 2 ASCII characters	Differentiated services code point for audio packets. Allowed values of 0 to 63.	CDG	0
DscpSignaling	Up to 2 ASCII characters	Differentiated services code point for audio packets. Allowed values of 0 to 63.	CFG	0
DtmfLevels	Up to 3 ASCII Characters	This specifies the DTMF level in dB of in-band tones sent from the phone to the network. The allowed values are -1 to -20. These are attenuation levels in dB, so -1 is louder than -20.	CFG	-10
Ethernet1	Up to 10 ASCII Character	Status of the 1st Ethernet Interface. Ethernet2 Status, Speed/Duplex Where: Status is 0 or 1 (disabled or enabled) Speed/Duplex is one of the following: • Auto • 10/FD • 10/HD • 100/FD • 100/HD • 1000/HD • 1000/FD	CFG,MAN	1,Auto
Ethernet2	Up to 10 ASCII Character	Status of the 2nd Ethernet Interface. Ethernet2 Status, Speed/Duplex Where: Status is 0 or 1 (disabled or enabled) Speed/Duplex is one of the following: • Auto • 10/FD • 10/HD • 100/FD • 100/HD • 1000/HD • 1000/FD	CFG, MAN	1,Auto
FontPixmap	Up to 32 ASCII Character	Name of the .bmp format file that contains the font pixmap. It is downloaded from the FTP server on boot. Format is windows .bmp 16 color except on the S6c where it is 256 colors.	CFG	"fontpixmap.bmp"
Font2Pixmap	Up to 32 ASCII Character	Name of the .bmp format file that contains the large font pixmap used by the U/dlt2 signal. It is downloaded from the FTP server on boot. Format is windows .bmp 16 color except on the S6c where it is 256 colors.	CFG	"font2pixmap.bmp"
FtpServers	Up to 255 ASCII Characters	A comma separated list of up to 2 FTP servers. If a server is unavailable the phone goes through the list until a working server is found.	DHCP, MAN	0.0.0.0
GatewayAddress	Dotted Decimal ASCII	Gateway address for the telephone.	DHCP, MAN	0.0.0.0

Table 6-7 Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
GreyLevels	Up to 3 ASCII Characters	Grey level setting for the middle grey levels on the IP530 and IP560 only. Low middle grey level may have the values: 0=1/4 1=1/3 2=1/2 High middle grey level may have the values: 0=1/2 1=2/3 2=3/4 Example; 1,2	CFG	1,1
IcmpArpTimeout	Up to 5 ASCII Characters	Number of seconds before routing table entries created by ICMP redirects are timed out of the routing table. If 0, then they never time out.	CFG	0
IconPixmap	Up to 32 ASCII characters	Name of the .bmp format file that contains the icon pixmap. It is downloaded from the FTP server on boot. Format is windows .bmp 16 color.	CFG	"iconpixmap.bmp"
Include	Up to 64 ASCII Characters	The file name that is specified is read and its contents included into the master configuration file. Files may be specified completely, or may include the variables $Hardware, $Country or $Language. The value of the Hardware Version (programmed into flash at the factory e.g. K01M01P01L01), Country or Language Parameter is substituted for $Hardware, $Country or $Language when the file name is created. For example: Include “Country_$Country.txt” with the Country parameter set to 3 would load in the file “Country_3.txt” This will permit parameters to be specified based on the Country and Language parameter values.	CFG	“”
IPAddress	Dotted Decimal ASCII	IP address to be used by the telephone.	DHCP, MAN	0.0.0.0
KeepAlive	Up to 3 ASCII Characters	Number of seconds to wait for an audit endpoint command before initiating the IP phone failover. If set to zero recovery procedures will never be started. Valid range is 0 to 999 seconds.	CFG	120
Language	Up to 3 ASCII Characters	This parameter specifies the Language that is used by the Include parameter to identify a particular file to include. May be between 1 and 255.	SSON, CFG, MAN	1
Layer2Audio	1 ASCII character	Layer 2 audio priority values from 0 to 7.	CFG	5

Table 6-7 Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
Layer2Tagging	1 ASCII character	802.1Q tagging enable on Port 1 0=Disable 1=Enable	SSON, CFG, MAN	0
Layer2Signaling	1 ASCII character	Layer 2 signaling priority values from 0 to 7.	CFG	0
MaxJitter	Up to 4 ASCII characters	The maximum value that the jitter buffer may be allowed to grow. Valid values are 10 to 300 mS in 1 mS steps.	CFG	50
MgcAuthenticate	Up to 1 ASCII Character	If enabled, then only authenticated MGC messages are accepted by the phone. 0=disable, 1=enable	CFG	0
MgcServers	Up to 64 ASCII Characters	Comma separated list of up to 2 MGC Servers. Must be in dotted decimal format. Example: 192.168.0.1, 192.168.0.2	SSON, CFG, MAN	0.0.0.0
MonthsOfYear	Up to 64 ASCII Characters	Comma separated list of the months of the year abbreviations used by the phone to display the time. First month is January.	CFG	Jan,Feb,Mar,Apr, May,Jun,Jul,Aug,Sep,Oct,Nov,Dec
NoSvc	Up to 64ASCII Characters	String that is displayed when the phone has lost service. Characters in this string must be specified using UTF-8.	CFG	“No Service”
OffHook	Up to 24 ASCII Characters	String that is displayed when the phone has been left offhook on the IP210. Characters in this string must be specified using UTF-8.	CFG	“Offhook”
PersistantEvents	Up to 255 ASCII Characters	Comma separated list of persistent events. Example: L/hu,L/hd, U/kd,U/ku	CFG	“”
ReqSvc	Up to 64 ASCII Characters	String that is displayed as the phone is waiting for service from the switch. Characters in this string must be specified using UTF-8.	CFG	“Requesting Service”
RingDefine	Up to 64 ASCII Characters	See the document "Custom Rings and Tones V4" for a definition of permissible values.	CFG	“”
RingMap	Up to 64 ASCII Characters	See the document "Custom Rings and Tones V4" for a definition of permissible values.	CFG	“”

Table 6-7 Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
RtpBase	Up to 5 ASCII characters	This is the base port from which the phone transmits and receives media. The valid range should be an even number from 3000 to 65408. 65408 is the highest even 16 bit number that allows enough headroom for the 64 RTP and 64 RTCP ports that are reserved when you establish an RTP base value. Given an RTP base, the phone should use the next 64 consecutive even numbers for RTP ports. If within that range an existing (reserved) odd or even UDP port number is used the phone should skip over an even/odd pair to the next even number. So, for example, if the user set rtpBase to 5550 we would use 5550, 5552, 5556, 5558, etc. In this example we skipped 5554 because 5555 is a reserved port used by the phonectl server (Actually 5554 is also used and also provides a reason for skipping over 5554). If an odd number is specified, the phone should use the next lowest even number if it fits the above limitations.	CFG	3000
SetupPassword	32 ASCII Characters	This is the MD5 hash of the password that must be entered after the mute button is pushed to enter a manual key command. Note that this password must be saved in flash after a value has been received from the MGC so it can be enforced on subsequent reboots. It is not cleared by the CLEAR command nor the clear step in the SETUP command.	MGCP	1234
SiteOption	Up to 3 ASCII Characters	Site-specific option number used by DHCP between 128 and 254.	CFG	156
SntpServer	Dotted Decimal ASCII	SNTP server address in dotted decimal format.	DHCP, CFG, MAN	0.0.0.0
SpeakerLevels	Up to 255 ASCII Characters	Set the audio levels of the speakerphone using a comma separated list of the following settings. The default values in decimal are listed next to the name for clarity. TxGain 4096 RxGain1 258 RxGain2 410 RxGain3 649 RxGain4 1029 RxGain5 1631 RxGain6 2584 RxGain7 4096 RxGain8 6492 RxGain9 10289 RxGain10 16306 Speaker DTMF Attenuation 13 Call Progress Tone Attenuation 13	CFG	See Description

Table 6-7 Phone Configuration Parameters

Parameter	Value Type	Value	Source	Default
SubNetMask	Dotted Decimal ASCII	Network Mask for the telephone. On boot, the phone checks for a non-zero NV value, and if one is present it is used.	DHCP, MAN	0.0.0.0
SysLogInfo	Up to 32 ASCII Characters	IP Address, module, verbose level, facility code, and output device of the SysLog function. The port number may be optionally identified and appended to the IP address. The default of 514 will be used if no port is specified. The module is a 32-bit integer where each bit refers to the debug enable/disable status from a specific software module. Bit assignments are defined in "Configuring Syslog Functionality for the ShoreTel IP Phones." The verbose level indicates the level of information that is printed. Levels are 0 to 7. Facility code is the syslog facility code. The output devices are 0= serial port, 1=syslog server. Example: 192.168.0.3:514, 279,33,1	CFG	0.0.0.0,0,0,0,0
ToneDefine	Up to 64 ASCII Characters	See the document "Custom Rings and Tones V4" for a definition of permissible values.	CFG	""
ToneMap	Up to 64 ASCII Characters	See the document "Custom Rings and Tones V4" for a definition of permissible values.	CFG	""
TouchBeep	0 or 1	If enabled the phone will play a beep when the touch screen is touched for user feedback.	CFG	0
Version	Up to 16 ASCII Characters	This parameter specifies the version identifier of the configuration file. It is then reported via the Mgc/gi signal request.	CFG	""
VlanId	Up to 9 ASCII Characters	VLAN ID to be used on tagged packets from the phone. Example: 1234	SSON, CFG, MAN	0
WallpaperPixmap	Up to 32 ASCII Characters	Name of the .bmp format file that contains the wallpaper pixmap. It is downloaded from the FTP server on boot. Format is windows .bmp 16 color.	CFG	"wallpaperpixmap.bmp"
WallPaper2Pixmap	Up to 32 ASCII Characters	Name of the .bmp format file that contains the user pixmap. It is downloaded from the FTP server on boot and when an Mgt/	CFG	"wallpaper2pixmap.bmp"
WaveRinger1	Up to 64 ASCII Characters	Used to assign one wave file to any of the ring signals. The first value is the signal, and the second value is the location of the file on the FTP server. Example: L/rg	CFG	""
WaveRinger2	Up to 64 ASCII Characters	Used to assign one wave file to any of the ring signals. The first value is the signal, and the second value is the location of the file on the FTP server. Example: L/rg 192.168.0.20/audio/dave.wav	CFG	""

Table 6-7 Phone Configuration Parameters

6.4.4 DHCP Site Specific Options

Parameters may be set from within a DHCP ACK message in the site specific option field (default is 156 but it may be modified with the **SiteOption** parameter). These parameters may be specified in the site specific option field:

FtpServers, Country, Language, Layer2Tagging, VlanId

Each parameter should be enclosed in quotes, and multiple parameters are separated by a comma. For example:

FtpServers=”192.168.0.13, 192.168.0.23”, Country=1, Language=1, SetupPassword=”12345abcde12345abcde12345abcde12”

6.4.4.1 Local Keypad Procedures

The phone supports the use of the keypad on the telephone to perform these procedures whenever it is inactive (handset and speaker inactive) or during the boot sequence before DHCP completes. If DHCP is turned off and manual settings are being used, the set should display the text "Password=?" and "Speaker= #=OK *=." for at least 1 second. The string assigned to **SetupPassword** (by the MGC server or the default) must be provided to access the SETUP command. All other commands are accessible without a password.

While the "Password?" prompt is displayed during the boot sequence the user may enter the muteINFO# (mute4636#) sequence to enter the local INFO command. When the INFO command is exited, the phone will again display the "Password" prompt and continue boot operations.

The SetupPassword will be sent by the MGC in hashed MD5 format. The telephone will compare the MD5 hash of the password the user entered with this value to see if the correct password has been entered.

On the IP phone models IP110/115/212k/230/530/560/560g, “Line 1” and “Line 2” in Table 6-8 refer to the top and bottom lines of the display. On newer models that support the programmable buttons feature, the display of these positions should be adapted to suit the capabilities of the LCD in use. The IP110 and 115 models are slightly different from the other models in that they have one line for displaying information. Thus, the “Line 1” information is scrolled across the LCD display and is followed by the more detailed “Line 2” information. (See Table 6-8 for clarification.)

The IP212k model has a narrow LCD display. Thus, the “Line 1” and “Line 2” information cannot fit on one line (as is possible with the other phones). Instead, the text must be wrapped around to appear on as many as 4 lines, for long strings.

If at any time during normal operation these sequences are entered, the operational display state is maintained while these commands are displayed, and the display is returned to the current state after the commands are finished (unless they require a restart).

While the phone is in any of these local key procedures, it returns an error code "501" indicating it is not ready, in response to any MGCP command received.

Because there is not a mute key on the IP110 phone, the transfer key on IP110 should be used instead of mute in the following access sequences.

6.4.4.2 Parameter Precedence

The active configuration of parameters used by the phone use the following order of precedence sources for all parameters:

1. Config file
2. DHCP (if active)

Access Sequence	Mnemonic	Procedure Description
Mute 4636#	INFO	Display the following information sequentially on the top and bottom lines of the display. All data is retrieved from the currently active configuration. Use * to exit and # to go to the next item. Phone returns to normal operation after the last screen. Line 1 — Line 2 IP Address Static/Dynamic — aaa.bbb.ccc.ddd Subnet Mask — aaa.bbb.ccc.ddd Gateway — aaa.bbb.ccc.ddd Link Speed — E1:A/1000/FDE2:M/1000/HD FTP Server — aaa.bbb.ccc.ddd MGC Server — aaa.bbb.ccc.ddd SNTP Server — aaa.bbb.ccc.ddd Tagging On/Off — VLAN ID=xxxx Application File — name Boot File — name Config File Date — mm/dd/yy hh:mm:ss a/p App Version — Build date Boot Version — Build date Country — # Language — # Model Number — # MAC Address — addr Serial Number — # Hardware Version — #
Mute 73887 #	SETUP	After the mute sequence is provided, if SetupPassword is not null, then prompt for the proper password ending in #. Do not display password digits as they are entered but use *. If a match, then prompt to "Clear All Values?". If no, then prompt for DHCP On/Off. If DHCP is on skip over the prompts for IP Address, Subnet Mask, and gateway. Then prompt for FTP Server, MGC Server, SNTP Server, Tagging On/Off, VLAN ID, Ethernet1, Ethernet2, Country, and Language. Save to NV storage if values are modified. If "Clear all Values?" is answered with yes, in addition to returning settings to the <Not Set> state, any cached DHCP values including the IP address are cleared. If a value was never configured using SETUP, it is displayed <Not Set> when its prompt is displayed. Otherwise, the value stored in flash is displayed. The only exception is the DHCP value which defaults and clears to the ON state. Setup value may be returned to the <Not Set> state by: • Answering yes to the "Clear All Values?" query • The factory CLEAR command (only executable from the serial port). All values are <Not Set> when the phone is new. This error checking should be performed on IP address entries during setup: • Only 0-9, * and # are accepted • Leading zeroes are ignored • Values outside 0-255 are ignored. If 2 digits are input, a 3rd digit that makes the value >255 is ignored. So upon entering 654, the 4 will be ignored. • Multiple "." Inputs are ignored • If no entry is provided before "." is entered, a 0 is automatically inserted.
Mute73738#	RESET	Display this warning before resetting the phone. On the top line "Reset Phone?" and on the bottom line "*=no #=yes".

Table 6-8 Local Command Interface

Access Sequence	Mnemonic	Procedure Description
Mute7464#	PING	The phone will prompt for an IP address and then ping that IP address 5 times and report the result after 10 seconds.
Mute25327#	CLEAR	A shortcut for enabling DHCP. Doesn't do anything else and is not password protected (only SETUP is). This command is present in the event someone hijacks the phone using the SETUP command. CLEAR allows it to be brought under DHCP control without knowing the password.

Table 6-8 Local Command Interface

3. Setup Command
4. Defaults

In other words, config parameters have precedence over DHCP over Setup over Defaults.

Not all parameter sources may be supported for every parameter. Table 6-7 indicates which sources are allowed for each parameter.

To fully manually configure a phone simply turn off DHCP, then use the Setup command but be sure not to specify an FTP server that might download a config file and overwrite your manual settings.

6.4.5 PhoneCTL Command Line Tool

PhoneCTL is a command line tool used to configure and diagnose ShoreTel IP phones. PhoneCTL commands can be run from the Windows command prompt.

Syntax for PhoneCTL commands can be obtained by typing `phonectl` at the prompt and pressing Enter.

There are several categories of commands available, including:

- Configuring syslog functionality for the IP phones
  - setLogLevel
  - setServerIP
  - setOutputDev
  - dump2pc
  - showLogLevel
- Retrieving information and statistics about phone connections
  - showConnInfo
  - showStats
  - showTime
  - version
- Troubleshooting data transfer issues between the phone and the syslog server
  - ifShow
  - arpShow
  - inetstatShow
  - ipstatShow
  - udpstatShow
  - tcpstatShow
  - hostShow
  - routeShow

All commands are case-insensitive.

After the ***phonectl*** command, the user is prompted to enter a password. After the user enters the correct password, the device permits access to executables that configure or diagnose the respective device.

CLI passwords are configurable only through Director. The default password is ShoreTel.

6.4.5.1 Configuring syslog Functionality for the ShoreTel IP Phones

Several commands are used to set up syslog functionality. These must be run before any logging messages can be received. The commands are as follows:

setLogLevel

The setLogLevel command sets the logging severity level. A log level remains in effect until a new setLogLevel command is issued.

Usage	`Prompt:\phonectl -setLogLevel [moduleID] [level] [destIP]`
Example	`Prompt:\phonectl -setLogLevel 3 7 192.168.0.170`
Parameters	`moduleID` is the ID number of the specific IP phone software modules the logging level is being set for. It is a 32-bit integer. Values must be 0—655335. Each bit in the integer enables or disables a specific module. Any module bit not set will not be logged. Hexadecimal values for ShoreTel phone software modules include: 0x1Call Processing (MGCC) 0x2Config File Processing (MCFGP) 0x4User Storage (MUSTG) 0x8Network Configuration (MNETC) 0x10User Interface (MELUI) 0x20Display Driver (MDIS) 0x40Provisioning (MPROV) 0x80Task Maintenance (MAINT) The number used in the parameter is the decimal equivalent of the sum of the hex values for all modules that are to be logged. For example, to turn on only the user interface module, enter 16 in the [moduleID] parameter (which is the decimal value of 0x10). To turn on call processing and config file process, enter 3 in the [moduleID] parameter (which is 0x1 + 0x2 in decimal). This is the value shown in the example command shown above. To turn on all modules, enter 255 (which is 0x1 + -x2 + 0x4 + 0x8 + 0x10 + 0x20 + 0x40 = 0x80). `level` sets the severity level to be logged. Values are 0—7, where zero is the most verbose. Levels are defined as follows: 0Emergency 1Alert 2Critical 3Error 4Warning 5Notice 6Informational 7Debug (This is the value set in the example shown above.) `destIP` is the IP address of the destination IP phone the command is sent to.

Table 6-9 setLogLevel Command

setServerIP

The setServerIP command sets the server's IP address and points to the location where messages are to be logged.

Usage	`Prompt:\phonectl -setServerIP [newServerIP] [destIP]`
Example	`Prompt:\phonectl -setServerIP 192.168.0.3 192.168.0.170`
Parameters	`newServerIP` is the address of the computer running the syslog server application. `destIP` is the IP address of the destination IP phone to which the command is sent.

Table 6-10 setServerIP command

setOutputDev

The setOutputDev command sets the output device to which the syslog messages are sent. The devise may be either a serial port or the syslog server.

Usage	`Prompt:\phonectl -setOutputDev [devID] [destIP]`
Example	`Prompt:\phonectl -setOutputDev 0 192.168.0.170`
Parameters	`devID` is set to zero if the device is a serial port or one for the syslog server. `destIP` is the IP address of the destination IP phone to which the command is sent.

Table 6-11 setOutputDev command

6.4.5.2 Retrieving Information about the IP Phone

dump2pc

The dump2pc command is used to retrieve the syslog messages from the ShoreTel IP phone's buffer. The results are printed to the command line.

Usage	`Prompt:\phonectl -dump2pc [destIP]`
Example	`Prompt:\phonectl -dump2pc 192.168.0.170`
Parameters	`destIP` is the IP address of the destination IP phone to which the command is sent.

Table 6-12 dump2pc

showLogLevel

The showLogLevel command prints the log level of each module for which logging is active. Information is printed to the command line.

Usage	`Prompt:\phonectl -showLogLevel [moduleNum] [destIP]`
Example	`Prompt:\phonectl -showLogLevel 4 192.168.0.170`

Table 6-13 showLogLevel command

Parameters	`moduleNum` is the IP address of the destination IP phone the command is sent to. `destIP` is the IP address of the destination IP phone the command is sent to. You will retrieve the log level settings for this phone.

Table 6-13 showLogLevel command

showConnInfo

The showConnInfo command shows information about connections created by MGCP_create messages.

Usage	`Prompt:\phonectl -showConnInfo [destIP]`
Example	`Prompt:\phonectl -showConnInfo 192.168.0.170`
Parameters	`destIP` is the IP address of the destination IP phone the command is sent to.

Table 6-14 showConnInfo command

showStats

The showStats command shows information about connections created by MGCP_create messages.

Usage	`Prompt:\phonectl -showStats [cxid] [destIP]`
Example	`Prompt:\phonectl -showStats 5 192.168.0.170`
Parameters	`cxid` is the ID number of a specific connection. The value can be discovered by reading the value returned by the showConnInfo command. `destIP` is the IP address of the destination IP phone the command is sent to.

Table 6-15 showStats command

showTime

The showTime command prints the time of day on the command line for the destination IP phone.

Usage	`Prompt:\phonectl -showTime [destIP]`
Example	`Prompt:\phonectl -showTime 192.168.0.170`
Parameters	`destIP` is the IP address of the destination IP phone the command is sent to.

Table 6-16 showTime command

version

The version command prints the version of the PhoneCTL software.

Usage	`Prompt:\phonectl -version`
Example	`Prompt:\phonectl -version`

Table 6-17 version command

6.5 ShoreTel Conference Bridges

The ShoreTel system interfaces with the ShoreTel Conference Bridge using IP phone ports to facilitate call control and media between the two systems. To the ShoreTel system, the ShoreTel Conference Bridge is 12, 24, 48, or 96 IP phones. The ShoreTel system has the same requirements for conference bridges as for IP phones.

The conference bridge uses MGCP to set up and tear down media streams between the ShoreTel system and the bridge. The conference bridge uses the G.711 codec for all conference calls.

The bridge must have one IP address statically assigned for each port supported by the bridge and one IP address for management and configuration access. These ports appear in the system as consecutively addressed IP phones.

The conference bridge IP ports are consecutive IP phone ports and are listed on ShoreWare Director's IP Phone List page. For more information, see the *ShoreTel Administration Guide*.

The conference bridge is assigned one number for users to dial into the bridge. Each port of the conference bridge is configured as a "user" in the system with an extension. Calls to the bridge are routed either by the call handling settings of the conference bridge ports (users) or by the ACD feature of a Workgroup. Incorrectly configured call handling can make conference bridge ports unavailable for calls. For reliability, ShoreTel recommends using call handling since it is switch dependant whereas Workgroup call handling is server dependant.

For more information, see the *ShoreTel Converged Conference Solution Administration Guide*.

6.5.1 SoftPhone

The ShoreWare SoftPhone is a Web-based application running from the ShoreTel server. The SoftPhone can be launched either from a URL supplied by the administrator or through Personal Call Manager. The SoftPhone is dependent on the server to start it up, but once launched it is no longer dependent on the server.

SoftPhone does not support NAT or firewall transversal. Problems with the Headquarters server or network connectivity can prevent the page from being loaded.

From a configuration and management standpoint, the SoftPhone appears to be an IP phone with some limitations. User have access to the DTMF keys (0-9, #, *), on hook, off hook, and flash.

The SoftPhone user interface does not have a display, so it does not interact with IPDS. Just like an IP phone, the SoftPhone uses MGCP for call setup and teardown, and RTP for media.

IP phones are uniquely identified by their MAC address. In most cases the SoftPhone is identified by the NIC of the user PC. If a SoftPhone is installed on a PC without a NIC, the SoftPhone generates a fake MAC address that is still unique.

The SoftPhone page contains an ActiveX control that implements the VoIP media support. Because it requires an ActiveX control, the SoftPhone only works on PCs with Internet Explorer and Microsoft Windows. The ActiveX object attempts to reach the switch call manager configured in ShoreWare Director. If a the switch call manager is successfully contacted, the SoftPhone buttons are enabled.

When the switch call manager is contacted, ShoreWare Director detects that a new IP phone is being registered. Depending on licensing and IP phone port availability, a new port is automatically created in the configuration database. The SoftPhone then appears in the Individual IP Phones list in ShoreWare Director.

If the Office Anywhere option is enabled, PCM waits for several seconds for a corresponding IP phone port to appear in the configuration database. If this times out, a warning message is displayed in the SoftPhone status bar.

When the SoftPhone or Personal Call Manager is closed, the Office Anywhere operation is reversed to return the user to his or her home port. Even if users are using the Office Anywhere feature somewhere else before invoking the SoftPhone, they are still returned to their home port.

6.6 Reference

6.6.1 Dial Tone Behavior

The following section discusses the dial tone behavior for various call operations and with different phones in the ShoreTel system.

Transfer

When a user is on a call and hits the transfer button, the phone will remain off-hook and will play dial tone. When the user completes the blind or consultative transfer while on the speakerphone or headset, the phone will automatically go on-hook. Only if a user is on the handset will the phone stay off-hook and play dial tone. A user using hands-free mode with speaker or headset will go on-hook without dial tone.

Park

When a user is on a call and hits the park button, the phone will remain off-hook and will play dial tone. When a user parks a call while on the speakerphone or headset, the phone will automatically go on-hook. The phone plays dial tone only if the user is on the handset. When using hands-free mode with the speaker or headset, the phone will go on-hook without dial tone.

Hold (in conjunction with multi-line IP phones: 212k/230/530/560/560g)

When a user on a multi-line IP phone places a call on hold while on the speakerphone or headset, the phone will go on-hook. Only if they are on the handset will the phone play dial tone (this feature is not 100% functional in the current ShoreWare build in Powerbar and will be fixed in the upgrade). A user using hands-free mode with speaker or headset will go on-hook without dial tone.

- To retrieve the call, go off-hook by lifting the handset, pushing the speaker button, pushing the headset button, or pushing the call appearance.
- To answer a second incoming call, press the second call appearance.
- To retrieve a second held call, press the second call appearance.

Hold (in conjunction with single-line IP phones: 110/115/210)

When a user on a single-line IP phone places a call on hold while on the speakerphone or handset, the phone will remain off-hook and will play dial tone. To retrieve a call, the user can go off-hook by lifting the handset and pushing the speaker button. A user using hands-free mode with speaker or headset will go on-hook without dial tone.

6.6.2 Manually Configuring the ShorePhone-IP100

The IP phones require configuration files in the *inetpub\ftproot* directory of the ShoreWare server. These files contain the configuration parameters and point to the application that is downloaded to the IP phone every time it boots. There is a master configuration file (00000000000.cfg) that provides the path to the phone application file and lists application files used to configure the phones.

Table 6-18 lists the configuration files and their function.

Type	Description	File Name
Default Master	The default master is the global master configuration file. Certain settings in the master configuration file are changed when you configure the system through ShoreWare Director.	000000000000.cfg
Baseline	These files contain global parameters that affect the basic operation of the IP phone, including voice codecs, gain, tone, and so on.	ipmid.cfg
Application	These files contain global parameters that set the basic mode of the application.	func.cfg
User	These files contain parameters that are unique to a particular phone user. Typical parameters include the user name and MAC ID of the IP phone. Each phone has its own customized version of this file identified by user name.	gmx<*user*>.cfg

Table 6-18 ShorePhone IP100 Configuration Files

ShoreTel 7 manages the configuration files for the IP phones. ShoreWare Director changes the contents of some configuration files according to the settings you make in Director. If you wish to modify the behavior of the IP phones via the configuration files, contact ShoreTel Customer Support.

6.6.3 Setting IP100 Phone Configuration from the Phone Interface

If you are not using a DHCP server, you must set configuration parameters from the IP phone's setup menu. You can also use the setup menu to set a custom Boot Server Option for the DHCP server and set the phone's VLAN identifier.

6.6.3.1 Accessing the Setup Menu

The setup menu is accessible when the IP phone boots. You can enter this menu during a six-second period, after which the phone enters normal operation using the current settings.

Rebooting the IP Phone

There are two ways to reboot the IP phone:

- By reapplying power
- By pressing four of the phone's keys simultaneously

The IP phone reboots whenever power is reapplied. You can accomplish this by disconnecting the power cable momentarily and then reconnecting it.

You can also reboot the IP phone by pressing four keys simultaneously. The four keys (as illustrated in Figure 6-1) are:

- Middle Blank Key
- Hold

- Volume –
- Volume +

Hold down these keys until the display shows that the IP phone is rebooting.

Figure 6-1 Reboot Keys on the ShorePhone IP Phone

During the boot process, the phone displays an option to enter the setup menu by pressing one of the soft keys (see Figure 6-2). To enter the setup menu, press the soft key below SETUP on the display.

6.6.3.2 Navigating the Menu Interface

You can navigate the menu interface using the IP phone keys shown in Figure 6-2.

a

Figure 6-2 Menu Keys

Table 6-19 explains the functions of these keys.

Key	Description
Scroll and Select	Use these keys to scroll through menu items and options. For some options, you can use the top and bottom arrow keys to skip to the first or last parameter in a range. The left-arrow key functions as a backspace key.
Soft Keys	The function of these keys changes with the current menu. The display shows the function of the active soft keys.
Alphanumeric keys	Use these keys and the soft keys to enter numbers and letters, such as for IP addresses and name strings.

Table 6-19 IP 100 Key Descriptions

6.6.3.3 Menu Options

The IP phone menu interface consists of the main setup menu and two submenus. The submenus set parameters for the Dynamic Host Configuration Protocol (DHCP) server and the ShoreWare server. You can scroll through menu options as described in the preceding section.

Table 6-20 describes the options available from the main menu in the order in which they appear.

Option Name	Value	Description
DHCP Client	Enable or Disable	Set to Enable by default. To configure TCP/IP parameters, disable **DHCP Client**.
DHCP Menu		If you are using the setup menu to modify the DHCP **Boot Server Option**, enter this menu. **DHCP Client** must be enabled.
Phone IP Address	Dotted-decimal IP address	The phone's IP address.
Subnet Mask	Dotted-decimal subnet mask	The phone's subnet mask.
IP Gateway	Dotted-decimal IP address	The phone's default router.
Server Menu		See Table 6-22 for ShoreWare server options.
SNTP Address	Dotted-decimal IP address	The SNTP server from which the IP phone obtains the current time (see "Configuring Time Source" on page 127).
GMT Offset	–12 through +13	The offset from Greenwich Mean Time in half-hour increments.
DNS Server	Dotted-decimal IP address	The primary server to which the IP phone directs Domain Name System queries.
DNS Alternate Server	Dotted-decimal IP address	The secondary server to which the IP phone directs Domain Name System queries.
DNS Domain	Domain name string	The IP phone's domain.
VLAN ID	0 through 4094	The IP phone's 802.1Q VLAN identifier.

Table 6-20 Main Menu options

Configuring Time Source

The configuration file for the IP100 phone (ip100.cfg), located in the *inetpub\ftproot* directory of the ShoreWare server. The line that needs to be modified is:

```
<SNTP tcpIpApp.sntp.daylightSavings.gmtOffset="-28800"
tcpIpApp.sntp.daylightSavings.enable="1"
tcpIpApp.sntp.daylightSavings.fixedDayEnable="0"
tcpIpApp.sntp.daylightSavings.start.month="3"
```

```
tcpIpApp.sntp.daylightSavings.start.date="8"
tcpIpApp.sntp.daylightSavings.start.time="2"
tcpIpApp.sntp.daylightSavings.start.dayOfWeek="1"
tcpIpApp.sntp.daylightSavings.start.dayOfWeek.lastInMonth="0"
tcpIpApp.sntp.daylightSavings.stop.month="11"
tcpIpApp.sntp.daylightSavings.stop.date="1"
tcpIpApp.sntp.daylightSavings.stop.time="2"
tcpIpApp.sntp.daylightSavings.stop.dayOfWeek="1"
tcpIpApp.sntp.daylightSavings.stop.dayOfWeek.lastInMonth="0"/>
```

The *gmtOffset* parameter represents the number of seconds offset from GMT: “-28800” is for Pacific Standard Time (PST), “-25200” is for Mountain Standard Time (MST), “-21600” is for Central Standard Time (CST), and “-18000” is for Eastern Standard Time (EST).

Configuring with DHCP

When DHCP is used to provide the IP address and configuration parameters to the telephone, the DHCP settings indicate which DHCP option is used to provide the ShoreWare server's address as the telephone's boot server. The settings configured in the telephones must match that of the DHCP server.

Option Name	Value	Description
Timeout	1 through 600	This value is the number of seconds the IP phone waits for secondary DHCP offers before selecting an offer.
Boot Server	Default, Custom, Static	When set to Default, the IP phone looks for option number 66 (string type) in the response sent from the DHCP server. The DHCP server must be configured to send the boot server address in option 66. When set to Custom, you specify the option number in the **Boot Server Option** field and the option type in the **Boot Server Option Type** field. The IP phone looks in the option having this number and type for its boot server. When set to Static, the IP phone uses the boot server configured through Server menu options. See Table 6-22.
Boot Server Option	128 through 254	When the **Boot Server** parameter is set to Custom, this parameter specifies the number of the DHCP option in which the IP phone looks for its boot server.
Boot Server Option Type	IP address, string	When the **Boot Server** parameter is set to Custom, this parameter specifies the type of DHCP option in which the IP phone looks for its boot server.

Table 6-21 DHCP Menu Options

Configuring without DHCP

When DHCP is not used to configure the telephone's boot server as the ShoreWare server, set the options described in Table 6-22 using the telephone's Server Menu.

Option Name	Value	Description
Server Type	FTP, Trivial FTP	When set to FTP, the IP phone uses the File Transfer Protocol (FTP) to obtain configuration and application files at boot time. When set to Trivial FTP, the IP phone uses the Trivial File Transfer Protocol to obtain configuration and application files at boot time. To configure the phone to use the ShoreWare server as its boot server, the Server Type is configured to FTP.
Server Address	Dotted-decimal IP address	This is the boot server used in any of the following: • If the DHCP client is disabled • If the DHCP server does not send a boot server address. • If the **Boot Server** parameter is set to Static. To configure the phone to use the ShoreWare server as its boot server, the Server Address is configured as the name or IP address of the ShoreWare server.
FTP User	Any string	When the **Server Type** parameter is set to FTP, this is the user name used when the IP phone logs in to the ShoreWare server. The default is `anonymous`. To configure the phone to use the ShoreWare server as its boot server, the FTP User setting must be configured to “ftp.”
FTP Password	Any string	When the **Server Type** parameter is set to FTP, this is the password used when the IP phone logs in to the ShoreWare server. The default password is `ftp`. To configure the phone to use the ShoreWare server as its boot server, the FTP Password should be configured to “shoretel”.

Table 6-22 Server Menu Options

CHAPTER 7

ShoreTel Client Applications

7.1 Overview

This chapter provides technical background information about the ShoreTel Call Manager application suite.

7.1.1 Call Manager Application Suite

The Call Manager suite includes:

- Different functional versions of the Call Manager client application: Personal, Professional, Workgroup Agent, Workgroup Supervisor, and Operator.
- Call Monitor software, including the Agent and Queue monitors.
- Viewer applications for Directory, History, and Voice Mail.
- Configure ShoreTel system, a control panel applet for configuring Shoreware clients.

7.1.2 Theory of Operations

All Call Manager applications are hosted within a single process named *STCHost.exe*.

TAPI objects manage all telephony-related data and tasks for Call Manager. Voice mail and database operations require CSIS. Call Manager applications use any available service and attempt to degrade gracefully if a requested service is unavailable.

A separate process (*STMapiRd.exe*) is invoked to load Microsoft Outlook contact data into the Call Manager's "white pages."

Only the Call Manager clients and three monitors (Extension, Agent, and Queue) can communicate directly with TAPI. All other applications must use Call Manager as a proxy to place calls on their behalf. Applications using Call Manager to dial calls are unable to provide feedback when an attempt to place a call fails. (However, notification of call failure does appear in the Call Manager application.)

7.1.2.1 Executable Modules

The table below provides descriptions of the top-level executable modules used by Call Manager applications.

Module	Description
StartCli.exe	Launches Call Manager application. (The application shortcut launches this task.)
STCHost.exe	Call Manager task.

Table 7-1 Call Manager Executable Modules

STCfgApp.cpl	Call Manager Control Panel application.
SendLogs.exe	Sends client logs to ShoreTel Customer Support.
STMapiRd.exe	Reads MAPI contacts and loads them into Call Manager.
CSISCMgr.exe	Client-side CSIS component.
TAPISRV.exe/ SvcHost.exe	Microsoft TAPI applications.
RPCTSP.TSP	TAPI Service Provider.

Table 7-1 Call Manager Executable Modules

7.1.2.2 Starting Call Manager Applications

All Call Manager applications are hosted from the process *STCHost.exe*, an out-of-process COM server.

To start a Call Manager client application, click the Call Manager application shortcut that appears on the desktop or Start menu. This starts *StartCli.exe*, opening Call Manager and any other applications left running when Call Manager was last exited.

7.2 Diagnostics

If a Call Manager application appears to be malfunctioning, use the following diagnostic guidelines to determine the point of failure.

7.2.1 Troubleshooting Login or Startup Problems

For the purpose of this discussion, login problems refer to issues related to CSIS.

The following symptoms may indicate login or startup problems:

- Double-clicking the application shortcut does not bring up the Call Manager main window.
- Call Manager appears, but no Call Handling Mode icon or Handsfree Mode icon is visible on the status bar/application tray. This is the most common symptom of login or startup problems.
- Agent Monitor appears, but fails to list agents.
- Extension Monitor appears and lists extension numbers, but without names.
- Voice Mail Viewer does not appear.
- Control Panel appears, but most fields are grayed out.
- Directory Viewer appears, but shows no data.

7.2.1.1 Missing Icons

Missing icons often indicate that CSIS was unavailable for user login.

The first time Call Manager successfully connects to CSIS, it stores a minimum amount of configuration data in the user's registry settings, including the user's current extension number; the values of the system extensions (AA, BAA, VM, VM Login); the values of the paging and night bell extensions for the user's site; and basic contact information (home country, home area code, and default access code).

This initial data store provides Call Manager with enough information to perform high-level tasks that include displaying call information and permitting the user to place and manage calls.

Normally, Call Manager locates the cached data and loads it while waiting for login to complete. After login, Call Manager updates the configuration information while it runs on the user's PC.

However, if CSIS is unavailable for login the next time the user starts Call Manager (or if the login fails), Call Manager uses the cached data until CSIS comes back online and login is successful.

The only time that a login problem can prevent Call Manager from launching is if the user has not run the application since installing or upgrading to the latest ShoreTel software release.

7.2.1.2 Login Problems

If a Call Manager application fails to log in, test the CSIS server to verify that it is running, check the login parameters, and open Windows Task Manager to confirm that no ShoreTel applications are running.

To troubleshoot login issues:

Step 1 Test the CSIS server.

Verify that the CSIS server is running by copying the following URL into your browser's address field.

(Change SERVERNAME to the name of the CSIS server.)

```
http://SERVERNAME/CSIS/CSISISAPI.dll/?request?00000000-0000-0000-0000-000000000000;CCSISSvrCONN::ping;
```

The browser window should display a result similar to this:

10;0x00000000;4;5440

Pay particular notice to the digits that appear after "0x."

If "x" is followed by a string of zeroes, the CSIS server is running.

If any digits other than zero appear after "x," you need to troubleshoot the ShoreWare server.

Step 2 Check the login parameters.

Open the Windows Control Panel, and click the Phone and Modem Options.

Click the Advanced tab to display a list of telephony providers.

Choose ShoreTel Remote TAPI Service Provider and click Configure.

The ShoreTel Remote TSP Device tab appears.

If the server name and/or login name are incorrect, continue with the sub-steps. Otherwise, skip to Step 3.

From the Provider Usage menu, choose Do not use this service provider (disable), and click Apply.

Change the server name and login name to the correct values.

From the Provider Usage menu, choose Use this service provider (enable), and click Apply.

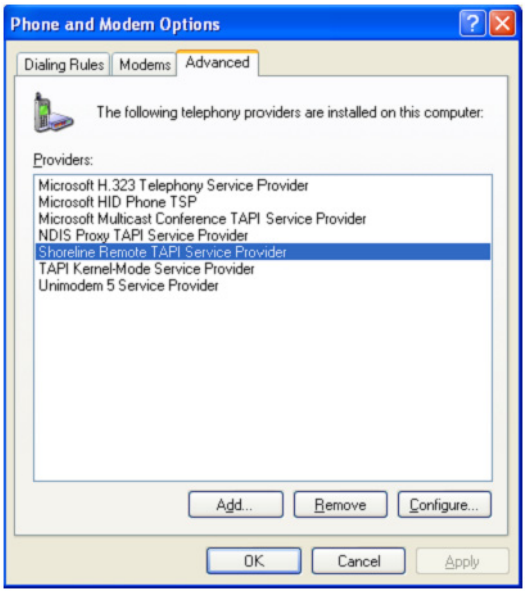

Figure 7-1 Phone and Modem Options, Advanced Tab

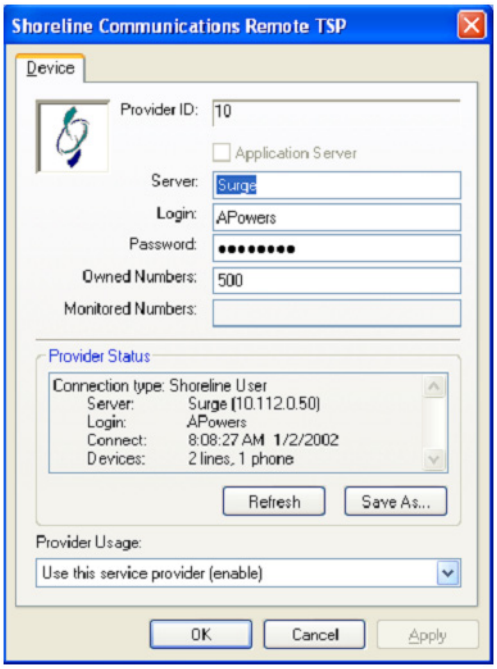

Figure 7-2 ShoreTel Remote TSP, Device Tab

Exit all ShoreTel applications. (Make sure *CSISCMgr.exe* exits. If it fails to quit, log out of Windows.)

Step 3 Open the Windows Task Manager and confirm that no ShoreTel applications are running.

If applications are running, use Task Manager to stop the applications in the order listed below. (If unsuccessful, wait for a brief period and try again.)

STCHost.exe

STMapiRd.exe

CSISCMgr.exe

7.2.2 Troubleshooting Telephony Problems

The following symptoms may indicate a telephony problem:

- On-hook/off-hook indicator is inaccurate.
- No call information is displayed for incoming calls.
- The user is unable to place an outgoing call.
- Nonexistent call information is displayed in the client.
- The user cannot perform a basic operation such as transferring an active call.

The following operations are useful in troubleshooting telephony issues.

7.2.3 Confirming TAPI Operations

The first task in troubleshooting telephony issues is to confirm that TAPI is functioning properly.

To confirm that TAPI is operating correctly:

Step 1 From a command prompt of the DOS window on the client PC, change the current directory to the *ShoreWare Client* directory and run the *tapitest.exe* test tool.

```
C:\Program Files\Shoreline Communications\ShoreWare
Client>tapitest
```

A listing of line devices appears, including a device displaying user statistics.

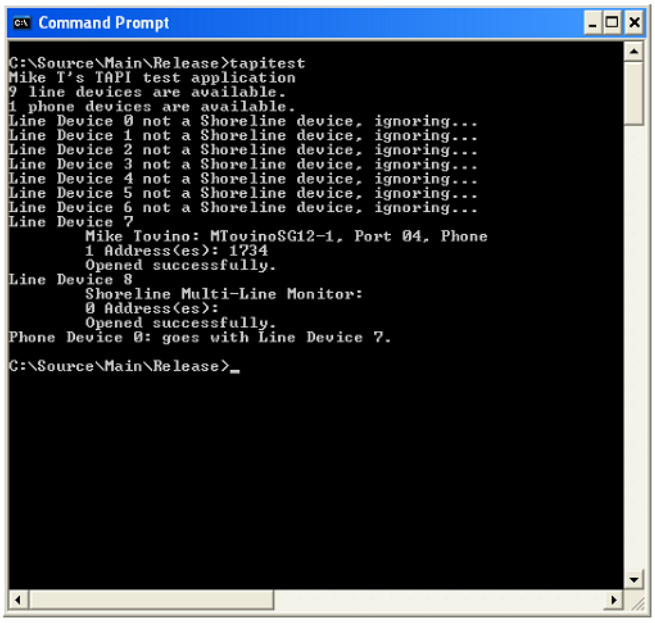
Command Prompt
C:\Source\Main\Release>tapitest
Mike T's TAPI test application
9 line devices are available.
1 phone devices are available.
Line Device 0 not a Shoreline device, ignoring...
Line Device 1 not a Shoreline device, ignoring...
Line Device 2 not a Shoreline device, ignoring...
Line Device 3 not a Shoreline device, ignoring...
Line Device 4 not a Shoreline device, ignoring...
Line Device 5 not a Shoreline device, ignoring...
Line Device 6 not a Shoreline device, ignoring...
Line Device 7
Mike Tovino: MTovinoSG12-1, Port 04, Phone
1 Address(es): 1734
Opened successfully.
Line Device 8
Shoreline Multi-Line Monitor:
0 Address(es):
Opened successfully.
Phone Device 0: goes with Line Device 7.
C:\Source\Main\Release>

Figure 7-3 Line Device Statistics

If no line device appears with the user statistics, TAPI is not working properly. Either the Call Manager was installed incorrectly, or the TAPI Service Provider has been removed or corrupted.

Reinstall the client software to correct the problem.

Step 2 Use the Windows phone dialer to confirm that TMS or Remote TSP is down.

Start the Windows phone dialer (*dialer.exe*).

From the Tools menu, choose Connect Using. If no entries appear in the Line drop-down list, or the only entries are modems or other locally installed telephony devices, either TMS or Remote TSP is not working.

If the drop-down list displays valid entries, confirm that one of the entries matches the user's switch port and extension.

If there is no match, the Remote TSP is configured improperly.

Reconfigure Remote TSP from the Telephony Applet in the Windows Control Panel, or by reinstalling the client software.

If the user's entry appears in the drop-down list, choose and attempt to place a phone call to the number with the dialer.

If the call fails, TAPI is only partially functioning.

If the call succeeds, TAPI is not the problem. Try restarting the Call Manager. If it still is not functioning, call ShoreTel Customer Support.

7.2.4 Troubleshooting Caller ID Problems

The following symptoms may indicate Caller ID issues:

- A call is displayed, but the Caller ID name and/or number is incorrect.
- Names and numbers listed in routing slips do not match what appears in the call display.

These problems can arise from any of these system layers:

- Call Manager
- Remote TAPI Service Provider
- TMS
- ShoreGear Switch
- Telephone Company Central Office

To isolate a Caller ID problem:

Step 1 Use another TAPI application, such as Phone Dialer or TB20, to check the connected ID name and number.

The name and number should match the information that appears in Call Manager.

If these do not match, it is probable that Call Manager detected the number in another application running on the user's machine and applied formatting rules to make the entry unique.

Step 2 Locate the call in question and use the *TMSncc* log to view the Caller ID information the client sent to the server.

Step 3 Use the trunk debugger to identify what the CO sent to the switch.

7.2.5 Troubleshooting Configuration Problems

The following symptoms may indicate configuration issues:

- A Server Unavailable message appears when the user attempts to change his or her call handling or headset mode.
- Unable to use **Configure ShoreTel System** via Call Manager's Options menu, or unable to access "ShoreTel System" from Windows' Control Panel.
- Call handling mode or headset mode display on Call Manager is inaccurate.

Review Section 7.2.1 on page 132. Most of the diagnostic guidelines in that section apply to configuration problems as well.

To isolate a configuration problem:

Step 1 Confirm that the CSIS server is running by entering the URL provided in the earlier section.

Step 2 If the CSIS server is running, make sure that *CSISCMgr.exe* is also running on the client PC.

Step 3 If the client process is running, try toggling the hands-free mode on and off, or change the call handling mode.

Step 4 Verify that Call Manager is connected to the CSIS server by placing the cursor in the QuickDialer dialog box and pressing CTRL + F12.

You should see a diagnostics dialog that you can use to check the connection.

7.2.6 Troubleshooting MAPI Contact Import Problems Using *SHAdrTst.exe*

You can isolate MAPI contact import problems by running *SHAdrTst.exe* (included on the client DVD).

To run *SHAdrTst.exe*:

Step 1 From a command prompt or DOS window on the client PC, run *SHAdrTst.exe*, by typing:

```
SHAdrTst
```

The command lists what Call Manager will import.

The table below lists available options for *SHAdrTst.exe*.

Command	Description
SHAdrTst > filename.txt	Transfer the output to a file.
SHAdrTst –debug -stdout	Include debugging statements in the output.
SHAdrTst –debug –stdout > filename.txt	Include debugging statement in the output file. The output lists all data imported by Call Manager.

Table 7-2 SHAdrTst.exe Options

7.2.7 Using the History File

Call Manager stores all history data in the text file *History.txt*, which is a valuable resource for troubleshooting application problems.

7.2.7.1 Locating the History File

The file is located in <*user app data*>\ShoreWare Client\<*username*>.

An example path:

```
C:\Documents and Settings\mtovino\Application Data\ShoreWare
Client\Mtovino\history.txt
```

On other platforms, the file is located in <*client install*>\<*username*>.

An example path:

```
C:\Program Files\Shoreline Communications\ShoreWare
Client\Mtovino\History.txt
```

The History file stores text in a tab-delimited format, making the file available for viewing with other applications such as Excel.

7.2.8 Using Log Files

Another critical resource for troubleshooting is the log file where Call Manager logs TAPI events, configuration events, and voice mail events, as well as all unexpected errors, exceptions, and warnings.

The main log file is named *CC-MMDDYY.log*. CC is literal and *MMDDYY* is a variable representing the month, day, and year. (For example, CC-061403.log). There are other log files, such as CSIS-MMDDYY.log, for other processes running on the client.

7.2.8.1 Locating the Log File

You can find the log file in <*app data*>\ShoreWare Client\Logs on most Windows machines, or <*install dir*>\Logs on other platforms. (See Section 7.2.7 on page 138 for examples of pathnames.)

7.2.8.2 Creating Verbose Logs

Generally, only unexpected errors are logged to the error log. You can change this priority from the QuickDialer if you want to create more detailed logs.

Use verbose logging only if a problem is reproducible and ShoreTel Customer Support requires additional information.

To turn on verbose logging:

Step 1 Position the cursor in the QuickDialer window and press CTRL + F12.

Step 2 Check the boxes for preferred types of logging. To ensure you capture as much logging information as possible, check all boxes except phone number parsing.

The resulting logs are voluminous.

Preset Debug Flags

You can preset debug flags by running *STClient –d* from the command line instead of *Stclient*.

7.2.8.3 Collecting Logs

To collect logs to send to ShoreTel Customer Support, use the SendLogs utility.

From the Start menu, go to *Programs/Shoreline Communications/Support/Send Client Log*s. A wizard guides you through the rest of the process.

7.3 Reference

7.3.1 Call Activity Log File

Call Manager saves all call activity logs to the file *history.txt*. (When users open the History Viewer application to view a call history, they are displaying log data read from *history.txt*.)

On servers running Windows XP or Windows 2003, *history.txt* is stored in the user's application data directory (ShoreWare Client/*<username>*). Under Windows 98 and Windows ME, *history.txt* is saved to a subdirectory in the ShoreWare Client install directory.

7.3.2 Customizing StartCli

The table below describes command line arguments you can use with *StartCli.exe* to run single applications or test modes.

Flags		Description
-cm		Runs Personal Call Manager.
	Option flags for Call Manager (append to *-cm* in any combination):	
	-n [*ext num*]	Runs Personal Call Manager against the specified extension in TAPI-only mode. No MAPI or CSIS connection is made. (Add MAPI connections via the *–o* or *–p* flag.)
	–d [*debug flags*]	Runs Personal Call Manager with the specified debug flags set, overriding the registry. No *-d* [debug flags] argument activates all the debug flags.
	–g [*level*]	Runs the Call Manager in GUI-only mode. The client does not make any TAPI, MAPI, or CSIS connections. This mode is useful for debugging painting issues. Level 1 is the full-featured GUI. Levels 2 and higher do not permit application docking.
	–j	Turns on just-in-time (JIT) monitoring (regardless of client type). The *-j* flag turns a Personal client into an Professional client. *–j x* adds Extended JIT info (call stack details and call handling details).
	–x	Provides access to the Extension Monitor, regardless of client type. Using *–j x –x* turns any client type into an Operator client. An Operator client invoked this way includes all Workgroup features as well.
	–l [*# seconds*]	Forces automatic exit from the client after the specified number of seconds. (Default value is 30 seconds.) This command flag is useful for running automated login/out tests when used in conjunction with *loginout_cc.bat.*
	–o	Activates Microsoft Outlook contact import, regardless of any other settings. Use this command flag in conjunction with *–n*.

Table 7-3 StartCli.exe options

	−p	Activates Microsoft Outlook contact import and popping, regardless of any other settings. Use this command flag in conjunction with *–n*.
-vm		Runs the Voice Mail Viewer. (A shortcut appears on Start menu.)
-cpl		Runs the Control Panel applet.
-amon		Runs the Agent Monitor.
-qmon		Runs the Queue Monitor. (Only if the user is a member of a workgroup.)
	Option flags for Queue Monitor:	
	−a	Shows all calls made against the Queue extension, not just those tagged as "queued" by the Workgroup server.
	−q [queue ext]	Runs against the specified queue extension. (Must be used with *–n*.)
	−n [*user ext*]	Runs client as the specified user. (Must be used with *–q*.)
	−d [*debug flags*]	Sets debug flags. If *–tes*t is not used, this flag sets debug flags for all applications running inside *STCHost.exe*.
-xmon		Runs the Extension Monitor.
-hist		Runs the History Viewer.
	Option flags for History Viewer:	
	-n [ext number]	Runs History Viewer as extension number. Use to read previously created history files in TAPI-only mode.
-stop		Shuts down all Call Manager applications. Use the flag to change users without logging off. (The flag does not shut down Microsoft Outlook or other MAPI applications.)
-test		Runs a specified application from within *StartCli.exe* instead of invoking *STCHost.exe*. Use the flag to run applications from the debugger and to isolate individual application processes. Note: *–test must* be the first argument in the command line.
-ShoreDevHelp		Displays a help screen of first-tier options.

Table 7-3 StartCli.exe options

7.3.2.1 Examples of *StartCli* Command Lines

Example 1: Runs Personal Call Manager in TAPI-only mode against extension 500.

```
StartCli -cm -n 500
```

Example 2: Same as above, but runs Call Manager with StartCli.exe instead of STCHost.exe.

```
StartCli -test -cm -n 500
```

Example 3: Make yourself an Operator using this command line.

```
StartCli –cm –j x –x
```

7.3.3 The Setup Wizard

Another component of the client, the Setup Wizard, continues the configuration of Call Manager after installation.

The Setup Wizard appears the first time Personal Call Manager runs on any PC. It reappears if a user cancels the Wizard before completing the configuration, or installs Microsoft Outlook at a later date.

The Setup Wizard starts if *any* of the following conditions are true:

- Any of the following string values are missing from (or blank in) the registry:
  - HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client\UserName
  - HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client\Server
  - HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client\Password
- The following *DWORD* value is missing from the registry:
  - HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client\LoadOutlookPhoneNumbers
- The following values are set to *TRUE* in the user row of the database *USER* table:
  - MustChangeGUIPassword
  - MustChangeTUIPassword
  - MustRecordName
- Microsoft Outlook is installed AND Voice Mail Outlook Integration is *not* installed AND the following *DWORD* value is missing from the registry, or set to *z* nonzero value:
  - HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client\OfferToInstallOutlookIntegration

If any of the specified conditions are TRUE, the Setup Wizard runs, while also setting one or more of the conditions to TRUE and starting the client.

Set the values only after exiting the client from the system tray and terminating *STCHost.exe*. Otherwise, exiting the client applications may overwrite the settings.

APPENDIX A

Event Codes

This appendix provides a comprehensive table of ShoreTel event codes. Organized by error type and sorted by event ID numbers, the tables are a valuable resource for troubleshooting events reported by the ShoreTel system.

A.1 Event Types

The tables list event types according to component functions of the ShoreTel telephony system:

- Switch
- TMS
- Voice Mail
- TDI Media
- Event Watch
- Configuration Administration
- Port Mapper
- Trigger Server
- Distributed Routing Service (DRS)
- Kadota Utility
- Call Accounting
- Workgroup Server
- CSIS
- IP Phone Console Server (IPCS)
- IP Phone Display Server (IPDS)

A.2 Using the Event Code Tables

In some cases, event codes result from other error conditions that cause related problems.

Always review event codes in the context in which they appear. For example, if event code 171 (internal operating temperature of switch is exceeding acceptable range) appears with code 166 (internal fan failure), it is likely that replacing the fan—and not the entire switch—will solve the problem.

A.2.1 Reading the Event Tables

The event tables in this appendix provide a structured view of events you may encounter in messages and log files.

Each event table entry includes a unique event ID number, a severity level, the event message text, possible causes, and suggested courses of action (if any).

A.2.2 About Severity Levels

Each event is assigned one of three levels of severity. The table below provides a guide to the severity levels in the tables.

Severity level	Explanation
Information	Reports status. Indicates normal operation, or a transition between normal operating states. Typically, no action is required.
Error	Reports an exception to normal operations. Depending on the event and its context with other events, it requires no action, monitoring, troubleshooting, or referral.
Warning	Alerts you to a failure or an impending failure—for example, when a service or hardware component is disabled. In most cases, a warning requires immediate response and resolution.

Table A-1 Severity Level Descriptions

A.3 Switches

ID	Severity Level	Message	Cause	Action
100	Error	Switch <*ShoreGear Switch Host Name*>: Event message lost, queue overflow.	The ShoreGear switch is receiving too many events from the NT Server. Possibly caused by an application problem on the ShoreWare server.	Check the ShoreWare server for events that might indicate an application problem. Troubleshoot the problem and reboot the server if you cannot identify a cause.
101	Warning	Switch <*ShoreGear Switch Host Name*>: The <area> in flash memory is corrupt and is being reset.	Flash memory area is corrupt.	If problem persists, return for repair.
102	Error	Switch <*ShoreGear Switch Host Name*>: Unable to reset <*area*> in flash memory, erase failure.	Application could not erase area of Flash memory.	If problem persists, return for repair.
103	Error	Switch <*ShoreGear Switch Host Name*>: Unable to update <*area*> in flash memory, write failure.	Application could not write area of flash memory.	If problem persists, return for repair.
105	Error	Switch <*ShoreGear Switch Host Name*>: Task exception occurred. System needs to be restarted.	A software exception occurred.	Contact ShoreTel Customer Support and be prepared to provide the log files for further analysis.
106	Error	Switch <*ShoreGear Switch Host Name*>: Task exception occurred. System automatically restarting.	A task exception has occurred. The ShoreGear switch experienced an internal error and is rebooting.	Contact ShoreTel Customer Support and be prepared to provide the *ipbx* and *tmsncc* log files for further analysis.
107	Information	Switch <*ShoreGear Switch Host Name*>: A restart request has been received—system is being shutdown and restarted.	The system administrator has restarted the ShoreGear switch via the Quick Look interface.	No action.
108	Error	Switch <*ShoreGear Switch Host Name*>: Internal error:	No longer reported in NT event log.	This event code reports internal software debug statements for use by ShoreTel developers.
109	Error	Switch <*ShoreGear Switch Host Name*>: Unable to seize trunk on port <*port number*>. Taking trunk temporarily out of service.	The switch cannot seize a trunk.	Verify the trunk line is connected to the ShoreGear switch. Check wiring between ShoreGear switch and the telephone company De-marc. Connect a phone or telephone test set to the line, then go off-hook and listen for a dial tone. If no dial tone is present, report the problem to your service provider.
110	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> has been taken out of service by the administrator.	The system administrator took the port out of service.	No action.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
111	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> is back in service.	The trunk line is again functional and has been placed back in service.	No action.
112	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> has been put back in service by the administrator.	The system administrator has put the trunk back in service.	No action.
113	Warning	Switch <*ShoreGear Switch Host Name*>: Extension on port <*port number*> has been taken out of service by the administrator.	The system administrator has removed the specified extension port from service.	Put the port back in service when the system administrator indicates that it is appropriate.
114	Information	Switch <*ShoreGear Switch Host Name*>: Extension on port <*port number*> has been put back in service by the administrator.	The system administrator has put the specified extension port back in service.	No action.
115	Information	Switch <*ShoreGear Switch Host Name*>: System has restarted. Product: ShoreWare Firmware Version: <*ShoreGear Switch firmware version number*> BootROM Version: <*ShoreGear Switch bootrom version number*> Telephone Board: <*ShoreGear Switch telephone board revision number*> CPU Board: <*ShoreGear Switch CPU revision number*>	The switch was reset and subsequently restarted. (The event also provides current version information for the switch.)	No action.
116	Error	<*ShoreGear Switch Host Name*> Lost connection to switch <*ShoreGear Switch Host Name*>.	The switch is unable to communicate with the other ShoreGear switch specified in the event. The switches will not be able to place calls to each other.	The specified switch may be off or disconnected from the network. Check the switch in question to confirm that it is powered on and connected to the network. If the switch is connected to the network, verify with Director that it is properly configured. For event 205 and 206 , update the configuration and power cycle the switch. After restart, confirm network visibility and the switch's configuration.
117	Information	Switch <*ShoreGear Switch Host Name* >: Established connection to switch <*ShoreGear Switch Host Name*>.	The switches established a connection and are communicating with each other.	No action.
119	Warning	Switch <*ShoreGear Switch Host Name* >: Excessive number of packets lost from <*ShoreGear Switch Host Name*>.	The switch is losing an excessive number of packets.	Verify that your network configuration meets ShoreTel requirements.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
127	Error	Switch <*ShoreGear Switch Host Name*>: Failed to forward call on <*CHM Type*> from <*extension number*> to <*extension number*>.	The call cannot be forwarded to the specified extension.	Confirm that the specified extension's call handling mode configuration is valid. This error can appear when the destination extension is connected to a ShoreGear switch that is either offline or unavailable to the network.
130	Error	Switch <*ShoreGear Switch Host Name*>: Failed to redirect incoming fax from <*extension number*> to <*extension number*>.	An incoming fax transmission call was not redirected to the fax extension.	Confirm that the extension is properly configured for fax redirection. Confirm that the fax extension is operating properly.
131	Error	Switch <*ShoreGear Switch Host Name*>: Extension <*extension number*> failed to acquire port <*port number*>.	The ShoreGear switch was unable to configure the specified extension on the desired port.	Reboot the switch. If this error persists, contact ShoreTel Customer Support.
132	Information	Switch <*ShoreGear Switch Host Name*>: Call restriction violation, call placed from <*extension number*> to <*dialed number*>.	The specified extension dialed a restricted number.	Inform user about dial-out restrictions.
138	Error	Switch <*ShoreGear Switch Host Name*>: Memory corruption detected - bad block <*parameter pinpointing failing block*> in partition <*parameter pinpointing failing partition*>.	A memory block corruption has been detected.	Reboot the switch. If the event persists, replace the switch.
140	Error	Switch <*ShoreGear Switch Host Name*>: Cannot re-initialize NvRam - Cannot Continue.	The flash memory in the ShoreGear switch is bad.	Replace the switch.
143	Warning	Switch <*ShoreGear Switch Host Name*>: Echo train grade F port <*port number*>.	The specified port did not receive proper echo cancellation properties. The trunk or phone connected to the port may exhibit poor sound quality or echo.	Use ShoreWare Director to reset the port. If the error was reported on a phone port, lift the phone's receiver to view the event log. (You may need to cover the mouthpiece to prevent ambient noise pickup.) If the error persists on a phone port, you may need to replace the phone.
144	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> has been connected for more than two hours.	The specified trunk has been connected to the port for two or more hours.	Confirm that an active call is in progress. If no call is present, reset the port from ShoreWare Director.
145	Warning	Switch <*ShoreGear Switch Host Name*>: Echo coeffs stuck possibly needs to be retrained port <*port number*>.	The echo suppression software was unable to adapt to a call in progress.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
146	Information	Switch <*ShoreGear Switch Host Name*>: Echo train grade A port <*port number*>.	The echo suppression software is properly configured.	No action.
147	Information	Switch <*ShoreGear Switch Host Name*>: Echo train grade C port <*port number*>.	The echo suppression software is properly configured.	No action.
148	Warning	Switch <*ShoreGear Switch Host Name*>: Low Erl possible hardware problem port <*port number*>.	The echo suppression software has detected a low echo-return loss on the specified port. This error can occur when modem or fax calls connect to a port. Event is infrequent and random.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.
149	Warning	Switch <*ShoreGear Switch Host Name*>: Low Erle port <*port number*>.	The echo suppression software has detected a low echo-return loss on the specified port.	No action for an isolated occurrence. If the error persists, follow the course of action suggested for Event 143.
151	Information	Switch <*ShoreGear Switch Host Name*>: Reboot due to configuration synchronization.	Reboot due to configuration change.	No action.
152	Warning	Switch <*ShoreGear Switch Host Name*>: DSP< *DSP number*> - 80% utilization.	The DSP on this switch is nearing capacity.	No action for an isolated occurrence.
153	Error	Switch <*ShoreGear Switch Host Name*>: DSP <*DSP number*> - 100% utilization.	The DSP on this switch has reached maximum capacity. In most instances, this event will not affect operations.	No action for an isolated occurrence. If the error persists, reboot the switch.
157	Error	Switch <*ShoreGear Switch Host Name*>: Received DHCP NAK for IP address <*IP Address*>.	The DHCP server has responded negatively to a DHCP lease renewal request. The IP address previously assigned to the switch is no longer available for that device. The DHCP server will assign the switch a new IP address.	In ShoreWare Director, display the Switches page and open the switch's record. Change the switch's IP address to the address assigned to it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the ShoreWare server.)
158	Warning	Switch <*ShoreGear Switch Host Name*>: DHCP lease expired for IP address <*IP Address*>.	The DHCP lease for the switch has expired and the switch is currently obtaining a new IP address. While the switch is obtaining another IP address, it will be unable to communicate with the ShoreWare server.	In ShoreWare Director, display the Switches page and open the switch's record. Change the switch's IP Address to the address assigned it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the ShoreWare server.)

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
159	Error	Switch <*ShoreGear Switch Host Name*>: DHCP IP address mismatch: <IP *Address*> Existing address: <IP *Address*> Offered address: <IP *Address*> Fatal Error... Rebooting <*ShoreGear Switch Host Name*>.	The IP address currently stored in the switch's flash memory is not the same as the address that DHCP is trying to assign to it. The switch will automatically reboot and obtain a new address.	In ShoreWare Director, display the Switches page and open the switch's record. Change the switch's IP address to the address assigned to it by the DHCP server. (You can use the Find Switches page if the switch is on the same LAN as the ShoreWare server.)
160	Error	Switch <*ShoreGear Switch Host Name*>: HAPI command failed. System automatically restarting.	The ShoreGear switch has experienced a fatal internal software error.	Contact ShoreTel Customer Support for updated information about fatal errors.
161	Error	Switch <*ShoreGear Switch Host Name*>: Connection to Telephony Management Server terminated - too many unacknowledged events.	The ShoreGear switch has stopped communicating with the TMS Server. This error can result from a CPU overload on the ShoreWare server.	Check the ShoreWare server for applications that are placing inordinate demands on the processor. Correct any application errors causing CPU overload.
162	Error	Switch <*ShoreGear Switch Host Name*>: Another device using the same IP address has been detected.	A device with the same IP address as the switch has appeared on the network.	Remove the offending device from the network, or ask the network administrator to assign the switch an alternate IP address.
163	Information	Switch <*ShoreGear Switch Host Name*>: Ethernet link established: using <*Ethernet speed*> <*Duplex mode*>.	The switch is connected to the Ethernet network.	No action.
164	Error	Switch <*ShoreGear Switch Host Name*>: Ethernet link lost.	The switch is no longer connected to the Ethernet network.	Confirm that network cables and ports are connected properly and are in working order.
165	Warning	Switch <*ShoreGear Switch Host Name*>: Receive pair polarity reversed.	The twisted pairing wiring for an ethernet cable is reversed.	Although the switch will continue to function, replace the suspect cable.
166	Error	Switch <*ShoreGear Switch Host Name*>: Fan failed.	The fan in the ShoreGear switch has failed.	Replace the ShoreGear switch.
167	Warning	Switch <*ShoreGear Switch Host Name*>: Fan running slow.	The fan in the ShoreGear switch is running slow. If the condition persists, the switch may overheat.	If this event is accompanied by Event 168, no action is required. If the error persists, replace the switch.
168	Information	Switch <*ShoreGear Switch Host Name*>: Fan running normally.	The fan in the switch is running normally.	No action.
169	Information	Switch <*ShoreGear Switch Host Name*>: Operating temperature: normal.	The internal operating temperature of the switch is within normal operating parameters.	No action.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
170	Warning	Switch <*ShoreGear Switch Host Name*>: Operating temperature: above normal.	The internal operating temperature of the switch is above the acceptable range.	Check if the event is accompanied by Event 166. If so, replace the switch. If the fan is working properly, check the environment in which the switch is operating to confirm that it is capable of supporting a temperature range within the switch's operating parameters.
171	Error	Switch <*ShoreGear Switch Host Name*>: Operating temperature: too hot.	The internal operating temperature of the switch has exceeded the acceptable operating range. The switch may soon fail.	Check if the event is accompanied by Event 166. If so, replace the switch. If the fan is working properly, check the physical location of the switch for environmental causes.
172	Error	Switch <*ShoreGear Switch Host Name*>: NvRam failure.	The ShoreGear switch was unable to write to the flash memory.	Reboot the switch. If the error persists, contact ShoreTel Customer Support.
173	Error	Switch <*ShoreGear Switch Host Name*>: VTALK failure.	The 48-Volt DC power supply has failed.	Replace the switch.
174	Error	Switch <*ShoreGear Switch Host Name*>: -70 Volt failure.	The 70-Volt DC power supply has failed.	Replace the switch.
175	Information	Switch <*ShoreGear Switch Host Name*>: Voltage OK.	The power supply that reported a failure is once again operating correctly.	No action.
176	Error	Switch <*ShoreGear Switch Host Name*>: Firmware Upgrade Failed: <*ShoreGear Switch Host Name*> <*specific diagnostic message*>.	The firmware upgrade for the switch has failed.	Check the switch event logs for subsequent appearances of Events 177 and 178. The presence of these events means that the switch has automatically recovered and you can ignore the alert of upgrade failure. If Events 177 and 178 are not also present, perform a manual upgrade of the firmware by rebooting the switch. If a reboot does not complete the upgrade, enter the *burnflash* command at the command prompt. This may indicate an installation problem.
177	Information	Switch <*ShoreGear Switch Host Name*>: Firmware Upgrade Started.	A firmware upgrade has begun.	No action.
178	Information	Switch <*ShoreGear Switch Host Name*>: Firmware Upgrade Finished	The firmware upgrade was successful.	No action.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
179	Error	1.5V too high: value = d.dV 1.5V too low: value = d.dV	Board failure	Return for repair.
180	Error	1.6V too high: value = d.dV 1.6V too low: value = d.dV	Board failure	Return for repair.
181	Error	2.0V too high: value = d.dV 2.0V too low: value = d.dV	Board failure	Return for repair.
182	Error	2.5V too high: value = d.dV 2.5V too low: value = d.dV	Board failure	Return for repair.
183	Error	3.3V too high: value = d.dV 3.3V too low: value = d.dV	Board failure	Return for repair.
184	Error	12V too high: value = d.dV 12V too low: value = d.dV	Board failure	Return for repair.
185	Error	25V too high: value = d.dV 25V too low: value = d.dV	Board failure	Return for repair.
186	Error	48V too high: value = d.dV 48V too low: value = d.dV	Board failure	Return for repair.
187	Error	75V too high: value = d.dV 75V too low: value = d.dV	Board failure	Return for repair.
188	Warning	Operating temperature: below normal	Temperature in room too cool.	Fix the environment.
189	Error	Operating temperature: too cold	Temperature in room too cold.	Fix the environment.
1300	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> has been connected for <*number of minutes*> minutes.	The trunk on the specified port was continuously active for the number of minutes specified. This message is generated after every two hours of continuous trunk activity.	Check the trunk and verify that an active call is in progress. If no call is present, reset the port from ShoreWare Director.
1301	Error	Switch <*ShoreGear Switch Host Name*>: Second TMS connection attempt from <*IP Address of second TMS server*>.	Another Shoreware Server has attempted to take control of the switch.	Only one ShoreWare server can control a switch; multiple servers cannot manage a switch simultaneously. Decide which ShoreWare server will manage the switch, then delete the switch from the other server.
1303	Error	Switch <*ShoreGear Switch Host Name*>: Configured IP <*IP Address*> does not match actual IP <*IP Address*>.	The IP address configured for the switch in Director is not the IP address the switch is using.	From Director, change the switch's IP address to match the address the switch uses.
1305	Information	Switch <*ShoreGear Switch Host Name*>: Free memory reduction trend. Min <*minimum memory used*>. Avg <*Average memory used*>.	Reports the switch's memory usage.	No action.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
1306	Warning	Switch <*ShoreGear Switch Host Name*>: Call could not be completed due to insufficient network bandwidth between sites.	An attempted call has exceeded the limit on the number of media streams allowed for multiple sites. May indicate the number of media streams configured for multiple-site calls cannot handle the inter-site call traffic.	From ShoreTel Director, open the Site Parameters page and check the number of media streams specified for the "Other Number of Media Streams for Multi_Site" parameter. Use the ShoreTel Site-Link Configuration Guide to determine the number of media streams the connection's bandwidth can support. If the bandwidth can support more media streams, raise the value specified for the site. Increasing the number of media streams may reduce sound quality for multiple-site calls.
1307	Information	Switch <*ShoreGear Switch Host Name*>: Trunk on port <*port number*> has been forced out of service.	Not reported in NT event log.	
1308	Warning	Switch <*ShoreGear Switch Host Name*>: T1 is in %2 loopback mode.	The T1 switch has been placed in either a local or payload loopback.	Your service provider is performing diagnostic tests.
1309	Information	Switch <*ShoreGear Switch Host Name*>: T1 is out of *%2* loopback mode.	The loopback on this switch has been removed.	No action.
1310	Error	Switch <*ShoreGear Switch Host Name*>: T1 framing error <*specific error*>.	The T1 switch is experiencing framing errors.	Check the cabling. Contact your service provider.
1311	Information	Switch <*ShoreGear Switch Host Name* >: T1 framing ok.	Framing has been restored.	No action.
1312	Error	Switch <*ShoreGear Switch Host Name*>: T1 signal error <*specific error*>.	The T1 switch has lost the T1 carrier signal.	Check the cabling. Contact your service provider.
1313	Information	Switch <S*horeGear Switch Host Name*>: T1 signal ok.	The T1 carrier signal has been restored.	No action.
1314	Error (Severity level varies depending on error)	Switch <*ShoreGear Switch Host Name*>: Config Store: <*specific error*>.	Notable event while reading non-volatile switch configuration.	No action. The configuration received from the server will supply any missing data.
1316	Information	Switch <*ShoreGear Switch Host Name*>: Trunk to trunk transfer from port <*port number*> has been killed after <*time interval*> of connection.	The system disconnected trunks on the reported ports as a result of option settings in Director.	No action.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
1317	Information	Switch <*ShoreGear Switch Host Name*>: ShoreTel Software Telephony Switch <*ShoreGear Switch*> Starting.	The ShoreTel SoftSwitch has started.	No action.
1319	Warning	Switch <*ShoreGear Switch Host Name*>: Emergency Services Call on port <*port*> from user <*user*> at <*ext or ani*>.	User called emergency number.	No action -- someone already called for help.
1320	Error	Switch <*ShoreGear Switch Host Name*>: SoftSwitch Cannot Start: Logger Failed.	The ShoreTel SoftSwitch failed to start because it could not contact the NT event log.	This message appears only after SoftSwitch has successfully contacted the NT Event Log Manager—meaning that the error condition has been cleared (possibly by the clearing of a full NT event log).
1324	Information	Switch <*ShoreGear Switch Host Name*>: Reboot due to configuration change.	Certain configuration changes, for example, changing signalling protocols for a SG-T1, requires a switch reboot.	No action.
1325	Warning	Switch <*ShoreGear Switch Host Name*>: A request has been received to reset the configuration and restart the system.	Can only be caused by issuing a command via *ipbxctl*. The command is only for use by ShoreTel support personnel.	This message confirms that SoftSwitch has stopped on command from the NT Service Manager. No action is needed.
1326	Information	Switch <*ShoreGear Switch Host Name*>: SoftSwitch Stopping *%*2.	The SoftSwitch service has stopped.	If the SoftSwitch service does not restart within two minutes, perform a manual restart and contact ShoreTel Technical Support.
1330	Error	Switch <*ShoreGear Switch Host Name*>: Soft Switch Stopping <*reason*>.	The SoftSwitch service has stopped.	If the SoftSwitch service does not restart within two minutes, perform a manual restart and contact ShoreTel Technical Support.
1331	Error	Switch <*ShoreGear Switch Host Name*>: Assertion failure %2	A software assertion failed.	If the problem persists, contact ShoreTel Customer Support and be prepared to provide the log files for further analysis.
1332	Information	Switch <*ShoreGear Switch Host Name*>: Trunk <*trunk*> received digits <*digits*> (no match), redirected to <*destination*>.	Incoming call on trunk failed to route.	Check trunk configuration.
1333	Information	Switch <*ShoreGear Switch Host Name*>: Trunk <*trunk*> received digits <*digits*> (too many), used <*number*>, redirected to <*destination*>.	Incoming call on trunk failed to route.	Check trunk configuration
1334	Information	Switch <*ShoreGear Switch Host Name*>: Trunks unavailable to route <*extension*> to <*dialed number*>.	Outgoing call failed due to no available trunks.	Verify that trunks are in-use.

Table A-2 Event Codes:Switches

ID	Severity Level	Message	Cause	Action
1338	Information	Switch <*ShoreGear Switch Host Name*>: Using PSTN failover to reach extension <*extension*> from extension <*extension*>, reason <*reason*>.	PSTN failover feature has been invoked.	Verify network connectivity between sites.
1339	Error	Switch <*ShoreGear Switch Host Name*>: <*message*>.	A request to record a call has failed.	If the problem persists, contact ShoreTel Customer Support and be prepared to provide the log files for further analysis.
1340	Warning	Switch <*ShoreGear Switch Host Name*>: <*message*>.	An attempt to conference using switch conference resources has failed.	Check switch configuration.
1341	Warning	Switch <*ShoreGear Switch Host Name*>: Call could not be completed due to insufficient network bandwidth at site <*site name*>.	Bandwidth limits have been exceeded.	Check site configuration.
1342	Error	Switch <*ShoreGear Switch Host Name*>: T1/E1 PRI D channel down.	PRI D channel down.	If the problem persists, contact PRI service provider.
1343	Information	Switch <*ShoreGear Switch Host Name*>: T1/E1 PRI D channel up.	PRI D channel up.	No action.
1344	Information	Switch <*ShoreGear Switch Host Name*>: SIP Dynamic Trunk Event: <*description*>.	Information about SIP trunk registrations.	No action.

Table A-2 Event Codes:Switches

A.4 TMS

ID	Severity Level	Message	Cause	Action
200	Error	TMS Assertion Failure: <*parameters*>.	TMS has encountered a non-fatal error.	Restart the TMS service. Contact ShoreTel Customer Support and submit a support incident.
201	Information	ShoreTel-TMS service started. Version: <*version number*>.	The TMS service has started.	No action.
202	Information	ShoreTel-TMS service stopped.	The TMS service has stopped.	No action. If the stoppage was unintentional, check the event logs for a cause.
203	Information	Updated switch <*ShoreGear Switch Host Name*> switch firmware to revision <*version number*>.	The switch has been upgraded to the version of firmware identified in the event.	No action.
204	Error	Failed to update switch <*ShoreGear Switch Host Name*> switch firmware to revision <*version number*>.	An upgrade to the switch's firmware failed. This switch will not operate properly until the firmware upgrade is complete.	Review the event log and correct any errors related to the upgrade failure. Reset the switch from ShoreWare Director. If the event persists, contact ShoreTel Customer Support.
205	Warning	Switch Ethernet Address to IP Address mapping change. Old Mapping: <*MAC Address*> <*IP Address*> New Mapping: <*MAC Address*> <*IP Address*> A telephony switch has been detected that has either changed it's IP address or is using an IP address previously in use by a different switch.	TMS has detected a configured switch that has had its IP address changed. The event reports previously assigned and current MAC and IP addresses for the switch.	Ensure the Switch <*MAC Address*> has been setup with a correct IP address. If the DHCP lease for the switch expires and the switch receives a new IP address. If this happens frequently, contact ShoreTel Customer Support.
206	Error	Switch Ethernet-Address IP-Address conflict. Expect: <*MAC Address*> <*IP Address*> Found: <*MAC Address*> <*IP Address*> A telephony switch has been detected with IP address or Ethernet address that is in conflict with the configuration database.	TMS has detected a switch with a MAC address and/or an IP address that conflicts with the address(es) configured for the device in ShoreWare Director. The conflicting address or addresses result from a misconfigured DHCP server or an incorrect switch record.	If address information was entered incorrectly for the switch, use ShoreTel Director to edit the record to include the correct address(es). (The switch reboots automatically when you save the record.) If the DHCP server assigned an incorrect IP address to the switch, correct the DHCP record and reboot the switch force reassignment of a new IP address.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
211	Warning	Switch <*ShoreGear Switch Host Name*> booted via FTP. Possible switch firmware corruption. A failure experienced during firmware upgrade will leave a switch booting via FTP instead of from its firmware.	The switch is no longer able to boot from flash memory and is now booting via FTP. The cause of the error is a failed firmware upgrade, bad firmware, or a reset caused by pressing the reset button.	Reburn flash memory. On the ShoreWare server, open a command prompt window and change the directory to the ShoreWare server directory (typical path is *Program Files\Shoreline Teleworks\ShoreWare Server*). Enter the *burnflash* command in this format: burnflash -s <IP address> (Use the IP address of the switch you are upgrading.) When the *burnflash* process is complete, check the event logs to confirm that the switch is no longer booting from FTP. If the event persists, replace the switch.
212	Warning	Switch <*ShoreGear Switch Host Name*> software version mismatch: TMS Version: <*TMS version*> Switch Version:<*ShoreGear Switch version*> The switch firmware will be upgraded the next time the switch boots.	TMS detects a switch with outdated firmware.	New switches ship with base firmware that is "down" from the current version. An automatic upgrade is confirmed when the device is put into service. (This event also appears during field upgrades.) From ShoreWare Director, open the Quick Look page and reboot the switch.
213	Error	Unexpected Ethernet address for switch <*ShoreGear Switch Host Name*> Expect:<*MAC Address*> Found:<*MAC Address*>. The switch is reporting an Ethernet address different from the one specified in the configuration database.	The MAC address in the switch's configuration record is incorrect.	From ShoreWare Director, open the switch configuration record and correct the MAC address.
214	Warning	Switch "<*ShoreGear Switch Host Name*>" firmware file version mismatch: TMS Version: <*TMS Version*> File Version: <*File version*> Cannot upgrade switch firmware. The firmware file used to upgrade the switch firmware does not have the correct version.	The firmware file *filessys.dll* does not match the TMS file version. The switch's firmware cannot be upgraded.	Re-install the ShoreWare server software. If the event persists, contact ShoreTel Customer Support.
221	Error	Failed to load firmware image file <*FileSys.dll*>. The Telephony Management Server was unable to load the switch firmware image file.	A switch firmware upgrade may not be possible.	This error appears when the "\Shoreline Communications\ShoreWare Server" does not have the "FileSys.dll" file, and TMS can't find or access this file. If this error appears frequently, contact ShoreTel Customer Support.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
223	Warning	Detected an unexpected configuration change. This may indicate that TMS was not notified of a change. The configuration inconsistency has been corrected.	TMS has corrected a configuration mismatch it detected on a switch.	No action. If this error appears frequently, contact ShoreTel Customer Support.
227	Information	ShoreTel-TMS service starting. Version: *<TMS version>*	The TMS service has started.	No action.
230	Warning	TMS was unable to find an TCP/IP network interface. This computer may not have a network adapter or may not be connected to a network. Operation will continue in stand-alone mode until the next TMS restart.	TMS failed to detect a network interface on the ShoreWare server.	Reboot the server. Troubleshoot the server's network configuration and make necessary repairs or modifications.
231	Error	The configuration for switch "*<ShoreGear Switch Host Name>*" no longer matches the system configuration database. This condition may exist on additional switches, and may result in unexpected behavior. Any switches shown to have a configuration mismatch in the Director-QuickLook page should be restarted to resolve the problem.	The configuration on the switch does not match the one stored on TMS. The mismatch can cause irregular behavior on devices connected to this switch. The error appears when there are network problems between the ShoreWare server and the switch, or is generated as a result of corrupted flash memory.	To synchronize the configuration data, reboot the switch. After the switch restarts, check the event log for messages that indicate network problems between the switch and the ShoreWare server to correct any network errors. If the event persists, check for events that indicate corrupted flash memory and and follow the instructions for correcting the problem.
233	Warning	TMS has disconnected from switch *"<ShoreGear Switch Host Name>"* (*<ShoreGear Switch IP Address>*). This may be as a result of a network outage, administrative action, or unexpected switch behavior.	TMS is reporting that it cannot communicate with the switch.	The disconnect is typically caused by a network-related problem such as outage or degraded performance. Correct the network problem. (The event also appears when the switch is taken offline for maintenance.)
234	Information	TMS has connected to switch "*<ShoreGear Switch Host Name>*" (*<ShoreGear Switch IP Address>*).	TMS has detected a switch and opened communications with the device.	No action.
235	Information	*<Connection type user or App Server>* TAPI connection for login *<user ID>* from *<IP address or name of system initiating the connection>* initiated.	A new TAPI connection has been accepted from a user at a specific IP address.	No action.
237	Information	TAPI connection for login *<user ID>* from *<IP address or name of system that is connected>* closed.	The TAPI connection to the specified user was closed.	No action.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
238	Warning	TAPI connection with login <*user ID*> from <*IP address*> denied access to extension <*Extension DN*>.	A user's remote TSP configuration tried to get ownership access to an extension the user does not own.	Contact the user and help him or her correct the client configuration.
239	Error	Attempting to connect to switch at IP address <*IP address*> with incorrect product type: Expected product type: <*Product Type ID*> Actual product type: <*Product Type ID*>. The configuration database has the incorrect product type for the switch at this IP address.	The switch at an IP address does not correspond to the switch type identified in the configuration database.	Edit the switch configuration information to reflect the correct data. Correct the IP address, or delete the switch, and create a new switch configured with the correct switch type.
241	Error	The Call Accounting Service returned the following error (<*Error code*>, Source = <*ShoreTel component that returned error*>): <*Message description*>.	TMS received an error code from the call accounting service in response to logged data.	Contact ShoreTel Customer Support and be prepared to provide server logs from the day of the occurrence. Note: This error is sometimes the result of a "false positive" and may not indicate serious problems.
243	Warning	TAPI request thread timed out after <*number of seconds*> seconds for context <*context handle ID*> performing request type <*request type ID*>.	TMS is not responding to internal messages in a timely fashion.	This event can precede a significant failure in TMS. Contact ShoreTel Customer Support and be prepared to provide server logs from the day of the occurrence.
244	Warning	<*Connection type user or App Server*> TAPI connection attempt for login <*user ID*> from <*IP address*> failed. Invalid <*LoginID*>.	A TAPI connection request was denied due to an invalid login or password.	Contact the user and assist him or her with login information.
246	Information	The Telephony Management Server has logged an informational debug message. The debug message contents are:<*Message*>	A logic assertion within TMS failed.	No action, unless the event is accompanied by system failures. If system failures are occurring, contact ShoreTel Support.
247	Information	The log file <*log file name*> current size is <*log file size*> bytes. It has exceeded its maximum size limit of <*max log size*> bytes. Further logging will be suspended.	The log file cannot write new events because it has reached its maximum size.	This event typically results from a configuration that creates an event loop. Review all configured call handling modes for loops. Example: UserA forwards calls to userB, who in turn is forwarding all calls to userA. If no logic fault is found, contact ShoreTel Customer Support.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
248	Information	Failed to write to the log file <*log file name*> (Error Code = <*error code*>). Further logging will be suspended until midnight or service restart. The ShoreWare log files collect diagnostics and are not required for correct system behavior.	TMS failed to write to a log files. (The embedded error code identifies the cause of the write failure.)	No action. Log files are not essential for telephony operations. If the problem persists, contact ShoreTel Customer Support.
249	Information	Failed to write to the log file <*log file name*> because another process has locked a portion of the file.	A write to the log file failed because the file was locked by another process.	This event can occur during normal backups of system log files. Local administrators can choose to suspend logging activity during scheduled backups.
251	Information	<*Connection type user or App Server*> TAPI connection did not give NEWCALL event (CallID = <*Call ID*>, Login: <*user ID*>, From: <*IP address*>). This may indicate a TAPI connectivity outage between the ShoreWare server and the telephony server on the machine specified.	When TMS notified a remote TSP of a new call, the remote TSP failed to accept or acknowledge that notification.	No action. If the event is accompanied by unusual client behavior, report the error to ShoreTel Customer Support.
252	Information	A time change of %1 was detected in the system clock.	The system clock was changed.	No action. Changing the system clock can result in inaccurate call timers for applications and skew call detail reporting records. A system clock adjustment only affects calls in progress at the time of the change.
253	Error	A rogue IP Phone Call Agent has been detected that has established a control connection with an IP Phone. IP Phone Details: IP Address:<*IP address*> MAC Address:<*MAC Address*> Call Agent Details:<*Call Agent Details*> Config'd Agent:<*Configured Agent*> Rogue Agent:<*Rogue Agent*>.	This error can occur when a Call Agent switch has been replaced and the previous switch is still on-line, or if an IP phone has been moved from one ShoreWare IP Phone System to another. This error can cause the IP phone to exhibit unexpected behavior.	Reconfigure the IP phone from the rogue Call Agent or take the rogue agent off-line. Typically this event occurs when two call agents attempt to control the same IP phone.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
255	Warning	The configuration database does not list this server as a configured ShoreWare server. The Telephony Management Services on this system will remain in stand-by and will not be fully available while this condition is present. The ShoreWare Director configuration of servers should be checked for correctness.	This server is not configured in ShoreWare Director as one of the ShoreWare servers; or IP addresses on this server do not match any of the configured IP addresses for servers in ShoreWare Director.	The administrator must configure this server correctly in ShoreWare Director and ensure the correct IP address has been given.
256	Warning	This server is configured with Loopback IP address. This may prevent other servers from reaching this server. Configure with proper IP address for this server.	ShoreWare servers cannot be configured with loopback IP addresses.	The administrator must configure this server correctly in ShoreWare Director and ensure the correct IP address has been given.
257	Error	The Telephony Management Service was unable to connect to or access the configuration database on the computer. Please ensure that network connectivity exists between this computer and the configuration database, and that the database services are operational on the main server. The Telephony Management Services on this system will remain in stand-by and are not fully available while this condition is present. The ShoreWare Director configuration of servers should be checked for correctness. (Error code = <*Error code*>).	This server is unable to connect to ShoreWare database on headquarters server.	The administrator must ensure there is network connectivity between this server and headquarters server. If the network connection is present and this condition persists, contact ShoreTel Customer Support.
258	Error	The main ShoreWare server has been configured in the configuration database with loopback IP address 127.0.0.1. Please ensure that proper IP address is configured for the main ShoreWare server. The Telephony Management Services remain in stand-by and will not be fully available while this condition is present. The ShoreWare Director configuration for the servers should be checked for correctness.	The main headquarters server has been configured with a loopback IP address.	The administrator must provide the correct IP address of the headquarters server.

Table A-3 Event Codes: TMS

ID	Severity Level	Message	Cause	Action
259	Information	The ShoreWare Telephony Management Service is reinitializing because new configuration changes have occurred. <Version of ShoreWare Server>	When administrator changes the IP address of a remote server, The ShoreWare Telephony Management Service on that remote server will be reinitialized with the new IP address. This event indicates the start of reinitialization process.	No action needed
260	Information	The ShoreWare Telephony Management Service is reinitialized with the new configuration changes. <Version of ShoreWare Server>	When the administrator changes the IP address of a remote server, The ShoreWare Telephony Management Service on that remote server will be reinitialized with the new IP address. This event indicates end of reinitialization process.	No action needed.
261	Warning	This ShoreWare Server has been deleted from the configuration database. Either this server has been deleted permanently or configuration changes have been made to this server that caused it to be deleted and added again. The Telephony Management Services on this server will be reinitialized and will remain in stand-by until the server is added again.	The ShoreWare Telephony Management Service will be reinitialized if configuration changes caused this server to be deleted and added again or it will remain in standby if this server is deleted.	If administrator has made the configuration changes that caused server to be deleted and added again, check the Quicklook page in ShoreWare Director to see if all the services running correctly. If not, please contact ShoreTel support.
262	Error	The configured IP address for this ShoreWare server has been changed in the configuration database. The Telephony Management Services needs to bind to new IP address and it will be reinitialized with the new IP address.	The IP address configured for this ShoreWare server has been changed in configuration database and ShoreWare Telephony Management service will be reinitialized with the new IP address.	The administrator has to check whether all the services are reinitialized correctly after IP address change. Check the Quicklook page in ShoreWare Director to see if all the services running correctly. If not, please contact ShoreTel support.

Table A-3 Event Codes: TMS

A.5 Voice Mail

ID	Severity Level	Message	Cause	Action
401	Information	Voice Mail Port Manager starting.Version: *<version number>*.	The Voice Mail Port Manager service has started.	No action.
402	Information	Voice Mail Port Manager stopping.	The Voice Mail Port Manager service has stopped. This error usually results from an intentional service stoppage, stoppage by a dependant service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for related errors and correct them. If necessary, restart the service.
410	Information	Recording stopped. The disk got full during recording.	A message was not completely recorded. The hard drive on which *\shoreline data\vms* resides is full.	Free up space on the drive.
411	Information	Recording stopped. The caller went silent during recording.	The person leaving a voice message was silent for more than 30 seconds, triggering automatic termination of the recording. The message is still sent so no action is required.	No action. The recipient will still be able to retrieve the partial message.
412	Information	Recording stopped. No response from the switch.	The recording of a message halted when the connection to the switch dropped.	Check the event log and correct any errors related to the dropped connection.
414	Error	The outbound AMIS phone number %1 for System ID %2 was a wrong number. No more attempts will be made to this system/number until it is corrected. Please verify the number is correct.		Verify that the phone number is correct.
415	Error	The outbound AMIS phone number for System ID %1 was not found. Please verify that the System ID has a phone number associated with it.		Verify that the System ID has a phone number associated with it.
416	Error	An internal error occurred. The system could not delete an AMIS message from the outbound message queue. System ID%1 Mailbox ID %2 Message ID %3		
417	Error	The undeliverable AMIS message from %2 could not be delivered to %3 for AMIS System ID %1. The message is being deleted.		

Table A-4 Event Codes: Voicemail

ID	Severity Level	Message	Cause	Action
418	Error	An error occurred during the delivery of an AMIS message from %2 to %3 for AMIS System ID %1, which prevents retrying delivery at a later time. The message has been deleted.		
419	Error	An error occurred during the delivery of an AMIS message from %2 to %3 (AMIS System ID:mailbox), and the system has tried %1 times to deliver this message. The message is being returned to the sender and deleted from the outbound queue.		
420	Error	An internal error occurred communicating between the Port Manager and another server. The error code was %1.		
421	Error	The number of delivery attempts (%2) to AMIS System ID %1 has been exceeded. Please verify the number is correct.		
1001	Information	Voice Mail Message Server starting. Version: <*version number*>	The Voice Mail Message Server service has started.	No action.
1002	Information	Voice Mail Message Server stopping.	The Voice Mail message service has stopped. This error usually results from an intentional service stoppage, stoppage by a dependant service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for related errors and correct them. If necessary, restart the service.
1003	Information	Voice Mail disk usage has reached maximum capacity.	A message was not completely recorded. The hard drive on which *shoreline data**vms* resides is full.	Take necessary action to free up space on the hard disk.
1004	Information	Voice Mail has no available messages stores.	The voice mail system cannot locate message storage directory *shoreline data**vms* on the ShoreWare server.	Verify that the hard drive or drive partition where *shoreline data**vms* resides is operating properly. Correct any disk problems and restart the server. If event persists, call ShoreTel Support.

Table A-4 Event Codes: Voicemail

ID	Severity Level	Message	Cause	Action
1005	Information	Voice Mail disk usage is greater than 90 percent.	The hard drive on which the message storage directory *\shoreline data\vms* resides is nearly full. When no disk space remains, Voice Mail will be unable to store new messages. This error appears once each day when the system disk is more than 90% full.	Free up disk space on the hard drive where *\shoreline data\vms* resides.
1006	Information	Error writing mailbox file to disk.	The Voice Mail system failed to a mailbox.dat file on the disk where the message storage directory *\shoreline data\vms* resides.	The write failure can result from corrupted data or a Windows NT error. Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server.
1007	Information	Error, disk got full when writing mailbox <*mailbox number*>.	The hard drive on which the message storage directory *\shoreline data\vms* resides is full. The mailbox a user attempted to create was not added.	Free up disk space on the hard drive where *\shoreline data\vms* resides.
1009	Information	Failed to get <*registry string*> from registry	Could not open required entry in the registry.	This may indicate an installation problem. Contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.
1011	Information	Voice Mail Message Server could not open message <*file name*> Error <*ShoreTel specific error*>.	The Voice Mail server could not retrieve a message because it was unable to read the disk.	Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server. If the error persists, contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.
1014	Information	Failed to attach message <*file name*> to mailbox <*mailbox ID*> Error <*ShoreTel specific error*>.	Error resulted from a failure with a specific mailbox.	This event results from a full mailbox included in a distribution list (or any other general failure related to a mailbox). Verify that the mailbox is full. If not, contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.

Table A-4 Event Codes: Voicemail

ID	Severity Level	Message	Cause	Action
1015	Error	All Voice Mail Message Server threads in use.	The mail server no longer has access to resources.	This event corresponds to a logged NT event indicating serious problems that can prevent clients from retrieving voice mail. Contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.
1016	Error	The system failed to send voice message <*file name*>.	The Voice Mail server failed to add a message to a user mailbox.	The probable cause is corrupted mailbox data. Verify that the mailbox is functioning properly. If not, contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.
1018	Error	The SMTP server used by voice mail is not sending messages.	The SMTP server is not forwarding stored messages on to recipients.	Verify whether the SMTP server is down, or if its address is set up incorrectly
1019	Error	A voice message sent to voice mail server <*file name*> has been returned.	A message sent to a remote server has been returned.	Contact ShoreTel Customer Support and be prepared to provide the voice mail log files for further analysis.
1020	Error	Failed to find entry in database for voice mail server.	A Voice Mail server looks up its own address in the database. The event indicates that the server could not locate a database record that matched its server name and/or IP address.	The probable cause is incorrect server information or incorrect IP address in the database. Edit the database record to include the correct data.
1101	Information	Voice Mail Application starting. Version: <*version number*>.	The Voice Mail Application service has started.	No action.
1102	Information	Voice Mail Application stopping.	The Voice Mail Application service has stopped. This error usually results from an intentional service stoppage, stoppage by a dependant service, or application failure.	No action if the service was intentionally stopped by a user. Otherwise, check the event log for event watch errors and correct them. If necessary, restart the service.
1109	Information	Could not create message <*message number*> Error <*error number*>.	The system could not write to the *mailbox.dat* file on the disk where the message directory *shoreline data**vms* resides.	A write failure is usually the result of corrupted data or a Windows NT error. Verify that the hard drive or drive partition where *shoreline data**vms* resides is operating properly. Correct any disk problems and restart the server.
1110	Information	Voice Mail disk usage has reached maximum capacity.	The hard disk drive or disk partition where the message directory *shoreline data**vms* resides is full. Voice mail will be unable to accept any new messages until disk space is made available.	Free up disk space on the drive where *shoreline data**vm*s resides.

Table A-4 Event Codes: Voicemail

ID	Severity Level	Message	Cause	Action
1111	Information	Removed <*file name*> millisecond message. Messages from callers must be at least <*configured limit*> milliseconds to send.	The message was too short to retain. Error is no longer logged.	
1112	Information	Message notification could not open phrase libraries.<*file name*> Error <*error number*>.	The voice mail system could not locate system prompts. The hard disk drive or disk partition where the message directory *\shoreline data\vms* resides is unavailable, was intentionally removed from the system, or is corrupted.	Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server.
1113	Information	There have been too many invalid logon attempts for mailbox <*mailbox number*>.	An attempt to log in to this mailbox has failed. While this event can indicate an unauthorized user, it most often results from a user who has forgotten (or mistyped) the password.	No action.
1114	Information	Listen unheard could not open message <*message number*>.	The server could not locate the indicated message number. The hard disk drive or disk partition where the message directory *\shoreline data\vms* resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server.
1115	Information	Listen saved could not open message <*message number*>.	The server could not locate the indicated message number. The hard disk drive or disk partition where the message directory *\shoreline data\vms* resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server.
1116	Information	Listen deleted could not open message <*message number*>.	The server could not locate the indicated message number. The hard disk drive or disk partition where the message directory *\shoreline data\vms* resides is unavailable or someone intentionally removed the message file from the system.	Verify that the hard drive or drive partition where *\shoreline data\vms* resides is operating properly. Correct any disk problems and restart the server.
1119	Error	The Voice Mail Application has determined that the Voice Mail Message Server is down.	Sending of voice messages has failed.	Restart mail server.

Table A-4 Event Codes: Voicemail

A.6 TDI Media

ID	Severity Level	Message	Cause	Action
2100	Information	ShoreWare Media Driver started.Version: <*Version Number*>.	The ShoreWare Media Driver has started.	No action.
2101	Information	ShoreWare Media Driver has stopped.	The ShoreWare Media Driver has stopped.	No action.
2102	Error	ShoreWare Media Driver failed to start. <*Message*>.	The ShoreWare Media Driver failed to start.	Contact ShoreTel Customer Support and be prepared to provide the NT system, and NT application log files for further analysis.
2103	Error	Failed to allocate non-paged pool memory. <*Message*>	The ShoreWare Media driver was unable to allocate non-paged pool memory. This failure can result in an inability to deliver media to IVR applications, and/or force a system restart with a crash dump.	Perform a system restart. Contact ShoreTel Customer Support and be prepared to provide the NT system application log files for further analysis.
2104	Information	Poor audio timer resolution. <*Message*>	The ShoreWare Media driver's internal timer detected an inaccuracy that was corrected.	No action. The event can indicate the occurrence of a voice-quality event that caused the driver to reset its internal timer.
2105	Error	Unable to map application buffer into kernal memory space. <*Message*>	The ShoreWare Media driver was unable to translate a user buffer to system memory. This failure can result in an inability to deliver media to IVR applications, and/or force a system restart with a crash dump.	If this error is appearing frequently, perform a system restart, In addition, contact ShoreTel Customer Support and be prepared to provide the NT system, and NT application log files for further analysis.
2106	Information	Recording of call was terminated due to silence. <*Message*>	The ShoreWare Media driver detected silence when recording a message. This may be due to incorrect behavior from one of the ShoreWare switches.	If this error is appearing frequently, perform a system restart, In addition, contact ShoreTel Customer Support and be prepared to provide the NT system, and NT application log files for further analysis.

Table A-5 Event Codes: TDI Media

ID	Severity Level	Message	Cause	Action
2107	Error	ShoreWare Media Driver is unable to bind all media channels within the configured UDP port range. Either the UDP port range given is not sufficient, or some of the UDP ports are being used by other components in this system. *<Configured UDP Range from registry for the Driver>*	The UDP ports to be used by the Media Driver can be configured using the registry by giving the range of UDP ports. ShoreWare Driver is unable to bind to the UDP ports given in the range.	The administrator must ensure that the UDP port range configured in the registry has at least 255 empty UDP ports, and reboot the server. Or this configuration option may be completely eliminated by removing the registry setting. This option enables the driver to choose any empty UDP port.
2108	Error	ShoreWare Media Driver is configured with invalid UDP port range. *<Configured UDP Range from registry for the Driver>*	The UDP ports to be used by the Media Driver can be configured using the registry by giving the range of UDP ports. The driver is configured with an invalid UDP port range.	The administrator must ensure that the UDP port range configured in the registry is between 1024 and 65535. After providing the correct UDP port range, the system must be rebooted.
2109	Warning	ShoreWare Media Driver has encountered an assertion statement that failed. In some cases an assertion failure may precede a more significant problem. The assertion statement details follow. *<Message description>*	A logic assertion in ShoreWare Media Driver failed.	If this error is appearing frequently, perform a system restart. In addition, contact ShoreTel Customer Support and be prepared to provide the NT system, and NT application log files for further analysis.

Table A-5 Event Codes: TDI Media

A.7 Event Watch

ID	Severity Level	Message	Cause	Action
1200	Information	The Event Watch service has successfully started.		No action.
1201	Information	The Event Watch service has successfully stopped.		No action.

Table A-6 Event Codes: Event Watch

A.8 Configuration Administration

ID	Severity Level	Message	Cause	Action
900	Information	User <*user name*> successfully logged in.	The specified user has logged into ShoreTel Director. A user history is maintained for auditing purposes.	No action.
901	Information	User <*user name*> failed to log in.	The specified user unsuccessfully attempted to log into ShoreTel Director. A user history is maintained for auditing purposes.	No action. (Monitor if the event persists.) While this event could indicate an unauthorized user is trying to access ShoreTel Director, it usually means that a user has forgotten (or mistyped) his or her password.

Table A-7 Event Codes: Configuration Administration

A.9 Port Mapper

ID	Severity Level	Message	Cause	Action
700	Information	<*ShoreTel-PortMap*> service starting. Version: <*version number*>	The Port Mapper service has started.	No action.
701	Information	<*ShoreTel-PortMap*> service stopping.	The Port Mapper service has stopped.	No action.
702	Error	Can't bind <*protocol type*> socket; port <*port number*> in use.	The preferred port for the RPC Portmapper (111) is already in use. Another network application or service is probably running on that system. While the port remains unavailable, no communication is possible between TMS and the switches.	Notify ShoreTel Customer Support, and be prepared to provide server log files.

Table A-8 Event Codes: Port Mapper

A.10 Trigger Server

ID	Severity Level	Message	Cause	Action
800	Information	<*Service name*> service starting. Version: <*Software version number*>.	The Trigger Server has started.	No action.
801	Information	<*Service name*> service stopping.	The Trigger Server has stopped.	No action.
805	Error	The notification server has lost connectivity with a notification client. This may indicate a network outage or unexpected client behavior. Client: <*name of affected service*> Status: <*error code*>.	Usually indicates that one of the ShoreWare services crashed without properly closing its connection.	No action, when related to a service failure. In other instances, check for network outages.
806	Error	The notification server has lost connectivity with the master notification server. This may indicate a network outage or unexpected behavior from the master *notification server.*	The connection between a Distributed Voice Mail Server and the HQ Server has failed.	No action, when related to a network outage or other administrative action. In the problem persists, collect log files from affected servers and contact ShoreTel Customer Support.
807	Error	The ShoreWare notification service on this server has received keep-alive message from an invalid client. The master notification may have already lost connection from this client. The client will reinitialize the connection back to master server (ShoreWare HQ server)	This event is sent to indicate flaky connection between ShoreWare notification services running on ShoreWare Remote Servers and ShoreWare HQ server	If this event is seen consistently, administrator has to make sure network connection between HQ server and remote server is up and running. If the problem still persists, please contact ShoreTel Support

Table A-9 Event Codes: Trigger Server

A.11 Distributed Routing Service (DRS)

ID	Severity Level	Message	Cause	Action
3100	Information	The Distributed Routing Service (Version %1) has started successfully.	The specified version of DRS has started.	No action.
3101	Information	The Distributed Routing Service has been stopped.	DRS has stopped.	No action.
3108	Information	The Distributed Routing Service reconnected to this switch: %n%1	DRS has re-established communications with the specified switch.	No action.
3109	Information	The Distributed Routing Service failed to connect to this switch: %n%1	Network connectivity may be lost to the specified switch, or the switch may be down.	Fix network connectivity issues, and confirm that the switch is up.

Table A-10 Event Codes: Distributed Routing Service (DRS)

A.12 Kadota Utility

ID	Severity Level	Message	Cause	Action
1400	Information	<*ShoreTel-KadotaUtil*> service starting. Version: <*version number*>	The specified version of Kadota Utility has started.	No action.
1401	Information	<*ShoreTel-KadotaUtil*> service stopping.	The Kadota Utility has stopped.	No action.

Table A-11 Event Codes: Kadota Utility

A.13 Call Accounting

ID	Severity Level	Message	Cause	Action
2000	Warning	TmsCdr records an attempt to archive an entry from table <*table name*> of <*database name*> to that of <*archive name*> with a duplicate <*duplicate ID*> primary key. It might be caused by a manual manipulation between CDR.mdb and its backup version.	During archiving, the call accounting service encountered a duplicate key value in a table. A duplicate value usually means the item has been archived previously. Results from renaming or moving the CDR database file without also renaming or moving the CDR archive database files.	Remove or replace the CDR archive database files.
2008	Information	ShoreTel-CDR service <*starting* or *stopping*>	Used to record service start/ stop events.	No action.

Table A-12 Event Codes: Call Accounting

A.14 Workgroup Server

ID	Severity Level	Message	Cause	Action
1600	Information	WorkgroupServer Started.	The workgroup server has started.	No action.
1604	Information	WorkgroupServer Stopping.	The workgroup server is stopping.	No action if server was stopped intentionally. Otherwise, review the WG*.log and SC*.log to identify reason for stoppage.

Table A-13 Event Codes: Workgroup Server

A.15 CSIS

ID	Severity Level	Message	Cause	Action
1898	Information	CSIS Web Services starting.		No action.
1899	Error	CSIS Web Services failed to start (<*error code*>).	CSIS Web services failed to start. (The embedded error code is a Microsoft error code.)	Contact ShoreTel Customer Support and be prepared to provide the CSIS log for review.
2400	Information	CSIS Web Services stopping.	CSIS Web services are stopping. (Occurs when web services are stopped.)	No action.
2401	Error	CSIS Web Services had an error (<*error code*>).	CSIS Web services experienced a non-fatal error. (The embedded error code is a CSIS or Microsoft error code.)	Contact ShoreTel Customer Support and be prepared to provide the CSIS log for review.
2402	Information	User <*username*> at Workstation <*workstation name*> authenticated.	The specified user is authenticated for CSIS server access.	No action.
2403	Information	User <*username*> at Workstation <*workstation name*> authentication revoked <***reason***>.	The specified user is no long authorized for CSIS server access. Causes include client logout, or an inactive connection as the result of a client who has gone offline without logging out.	
2405	Information	CSIS Web Services execution enabled.	CSIS Service has started. Client access to CSIS Services is enabled.	No action.
2406	Warning	CSIS Web Services execution disabled.	CSIS Service has stopped. Client access to CSIS Services is disabled. (Web services will continue to run.)	No action. The event is assigned a severity level of "warning," because a service (CSIS) is disabled and no longer accept logins or requests. But the result is "non-destructive"; the service can be enabled at any time.

Table A-14 Event Codes: CSIS

A.16 IP Phone Console Server (IPCS)

ID	Severity Level	Message	Cause	Action
2700	Information	ShoreWare IPCS Server started.	The IPCS Server has started.	No action.
2701	Error	Handler not installed.	The service was not installed properly.	Re-install the service.
2702	Information	The ShoreWare IPCS Server Stopped.	The IPCS Server has stopped.	No action.
2703	Information	Bad Service Request.	The service is not running.	Re-install the service.
2704	Information	Maximum capacity for Switch ID: <*switch identifier*> has been reached.	The switch has reached its maximum capacity of IP phones.	To support more IP phones, configure a new switch or add additional IP Ports to existing switches.
2705	Information	IP-Phone could not be configured. No switches are available on Site: <*site name*> The existing switch(es) have reached maximum capacity or may be temporarily down.	Switches at the destination site have reached maximum capacity of IP phones.	To support more IP phones, configure a new switch or add additional IP Ports to existing switches.
2706	Information	IP-Phone could not be configured. No IP Phone switches are configured on Site: <*site name*>.	No switches are configured to support IP phones at the destination site.	To support more IP phones, configure a new switch, or add additional IP ports to existing switches.
2707	Information	The IP Address for IP-Phone Device: <*MAC address of phone*> has been set to NULL in the configuration database.	The IP address for a "downed" IP phone has been set to NULL. This usually indicates that a new IP phone has appeared on the system using the same IP address as the phone that is "down."	No action.
2708	Information	The IP-Phone Device: <*MAC address of phone*> could not be configured since another IP Phone device is using the same IP Address.	The IP address assigned to an IP phone is already in use by another IP phone. The new phone cannot be configured.	Troubleshoot the DHCP server to determine why it is assigning the same IP address to two different phones.

Table A-15 Event Codes: IP Phone Console Server (IPCS)

A.17 IP Phone Display Server (IPDS)

ID	Severity Level	Message	Cause	Action
2800	Information	The ShoreTel IP Phone Display Service (*Version x.x.xxxx.x*) has started successfully.	The IPDS service has started.	No action.
2801	Information	The ShoreTel IP Phone Display Service has been stopped.	The IPDS service has been stopped.	No action.
2802	Error	The ShoreTel IP Phone Display Service (*Version x.x.xxxx.*x) has encountered a fatal error during startup; the service will be terminated.	The IPDS service crashed upon startup. (This is a fatal condition.)	Contact ShoreTel Customer Support and be prepared to provide server logs.
2803	Warning	An unexpected service control message <*Message ID as hexadecimal integer*> was encountered.	The Win32 Service Control Manager reports an unexpected message. The IPDS installation has probably been modified manually by the user.	Contact ShoreTel Customer Support and be prepared to provide server logs.
2804	Warning	An unexpected exception was encountered and handled. Exception description <*Description here*>.	An exception occurred and was handled by the logging of the error. Typically, one or more of the phones are displaying anomalies; a display update may not have been sent or a phone display is out of sync.	Contact ShoreTel Customer Support and be prepared to provide server logs. If users are experiencing problems, perform an administrative restart on the phones.
2805	Error	An unhandled exception was encountered. Exception description: <*Description here*>.	An exception occurred, but was not handled.	Immediately notify all IP phone users and restart IPDS to restore normal service. (Use the Send Diagnostic Message to dispatch a message to all phone displays.) Contact ShoreTel Customer Support and be prepared to provide server logs.
2806	Warning	The following warning condition was encountered in the ShoreTel IP Phone Display Service: <*Warning description*>.	A general error message that can indicate minor user problems. Usually the result of a non-fatal TAPI error.	Contact ShoreTel Customer Support and be prepared to provide server logs.
2807	Error	The following error condition was encountered in the ShoreTel IP Phone Display Service: <*Error Description*>.	A general error message that can accompany extensive user problems. Usually the result of a fatal TAPI error.	Contact ShoreTel Customer Support and be prepared to provide server logs. Perform other diagnostics at your discretion.
2808	Information	The phone display was reinitialized because of an administrative request: Extension: <*Extension number*>.	An administrator has reset the display on the phone at the specified extension.	No action.

Table A-16 IP Phone Display Server (IPDS)

ID	Severity Level	Message	Cause	Action
2809	Information	The phone display was reinitialized because of an administrative request: Port ID: <*Port ID*>.	An administrator has reset the display on the phone configured for the specified port.	No action.
2810	Information	All phone displays were reinitialized because of an administrative request.	An administrator has reset the display on all IP phones.	No action.
2811	Information	The phone display was reinitialized because of an administrative request: IP Address <*IP address*>.	An administrator has reset the display on the phone having the specified IP address.	No action.
2812	Warning	The IP Phone Display service encountered an apparent crash in the Microsoft Telephony Service. IPDS will attempt to recover from this problem. If users report anomalous behavior, you should stop and restart the Microsoft Telephony Service and all ShoreWare services that depend on it.	Fault in Microsoft Telephony Service; there is potential to recover automatically.	Watch for anomalous behavior. Restart the following if problems persist: • TMS • IPDS • Workgroup • All Voice Mail Services
2813	Error	The IP Phone Display service was unable to recover from an apparent crash in the Microsoft Telephony Service. You should stop and restart the Microsoft Telephony Service and all ShoreWare services that depend on it.	Fault in Microsoft Telephony Service; there is no potential to recover automatically.	Restart the following if problems persist: • TMS • IPDS • Workgroup • All Voice Mail Services
2814	Warning	The following config option was set to a value that is only intended for engineering use: <*option name*>.	An administrator has set a debug flag in the registry that was only intended for use by ShoreTel engineers.	Unset the option listed in the event message.
2815	Warning	The IP Phone display service is unable to connect to the ShoreTel database. It will retry in 30 seconds. <*error code that was encountered*>	IPDS was unable to access the database upon startup. It will try again in 30 seconds. No action need be taken at this time.	Also see 2816 and 2817.

Table A-16 IP Phone Display Server (IPDS)

ID	Severity Level	Message	Cause	Action
2816	Error	The IP Phone display service is unable to connect to the ShoreTel database. It will continue to retry once every minute. <*error code that was encountered*>	This only happens 30 seconds after a 2815 error, in the event that the retry for 2815 failed. At this point, the most common cause is that the most recent installation or upgrade on the server where the even t is generated did not properly register the ShoreTel database access libraries.	Unless the error is recovered from (see error 2817), this should generate a support call.
2817	Information	The IP Phone display service's connection to the ShoreTel database has recovered from the previous error.	A database retry after 2815/ 1816 errors was successful and the situation has been recovered from.	No action.
2818	Error	The ShoreTel database is missing a table or stored procedure needed to run the following stored procedure: (name if query). This will cause degraded functionality in IPDS. Please ensure that the HQ server and all Remote servers are running the same version of ShoreTel software.	The database file has been corrupted or a query has been removed or otherwise cannot be accessed at this time.	Call support.

Table A-16 IP Phone Display Server (IPDS)

APPENDIX B

DCOM Permissions

B.1 Introduction

ShoreTel systems have one HQ server and multiple remote servers. Applications running on remote servers access data service components residing on the HQ server through DCOM. DCOM permissions are configured by the Installer when the servers are installed and by the SP1Repair command line utility.

The following service logon accounts are available in Windows.

- **Local System account**: This account has full system access, including the directory service on domain controllers. Services logged onto the Local System account on domain controllers can access the entire domain. Some services log onto the Local System account by default. Do not change default service settings.
- **Local Service account**: This account is similar to authenticated user accounts. Services logged onto the Local Service account have the same access rights as members of the Users group and access network resources as null sessions with no credentials.
- **Network Service account**: This account is similar to authenticated user accounts. Services logged onto this account have the same access rights as members of the Users group and access network resources through the credentials of the computer account.

Figure B-1 displays the registry key settings.

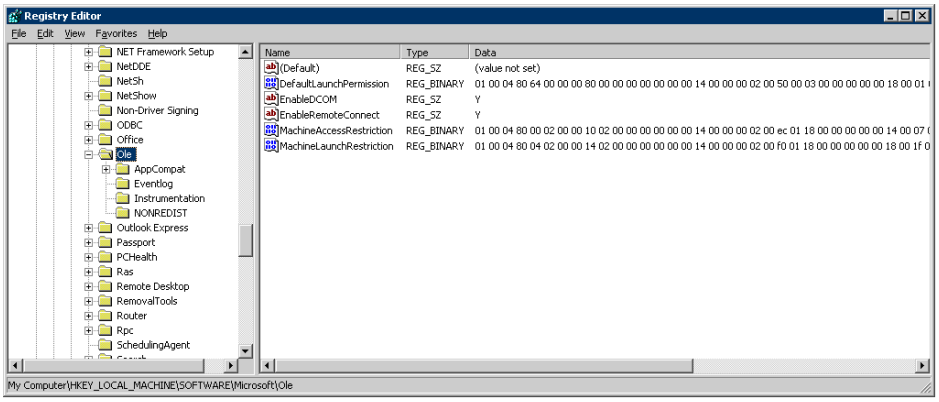

Figure B-1 Registry Keys modified by the Installer and the Sp1Repair Tool

B.2 Editing DCOM Permissions

DCOM permissions are modified on the HQ system through user interface actions listed in the following sections.

B.2.1 My Computer Properties

Open the **My Computer Properties** panel by selecting *MMC -> Component Services -> Computers -> My Computer -> Properties.*

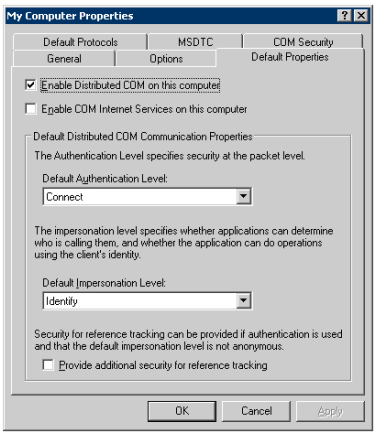
My Computer Properties
Default Protocols
MSDTC
COM Security
General
Options
Default Properties
Enable Distributed COM on this computer
Enable COM Internet Services on this computer
Default Distributed COM Communication Properties
The Authentication Level specifies security at the packet level.
Default Authentication Level:
Connect
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.
Default Impersonation Level:
Identity
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.
Provide additional security for reference tracking
OK
Cancel
Apply

Figure B-2 My Computer Properties window – Default Properties panel

Step 1 Open the **Default Properties** panel (Figure B-2).

Select *Enable DCOM*.

Step 2 Open the **COM Security** panel.

Step a Click *Edit Default* in the **Access Permissions** section.

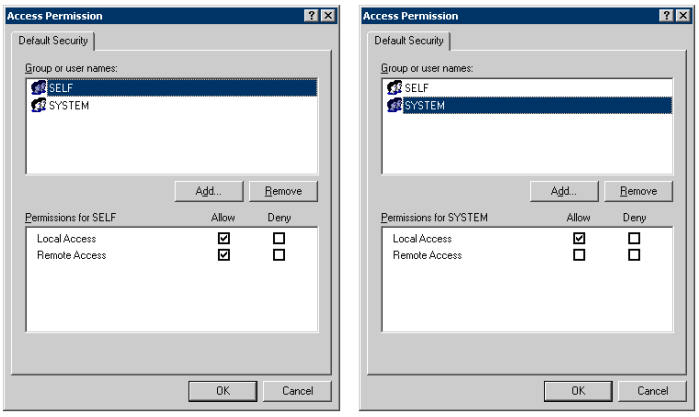

Figure B-3 Access Permission panel (My Computer Properties)

Select the following permissions, as shown in Figure B-3:

- SELF: Local Access – allow; Remote Access – allow
- SYSTEM: Local Access – allow; Remote Access – no selection.

Return to the **My Computer Properties** window by clicking *OK*.

Step b Click *Edit Default* in the **Launch and Activation Permissions** section.

Select the following permissions, as shown in Figure B-4:

- Administrators: Local Launch – allow; Remote Launch – allow
  Local Activation – allow; Remote Activation – allow

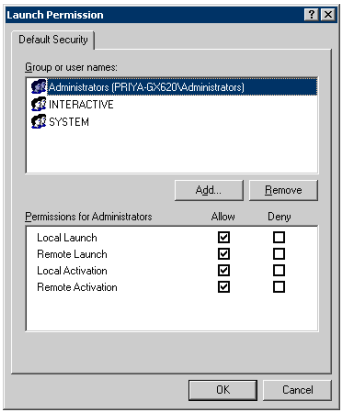

Figure B-4 Launch Permission panel (My Computer Properties)

- INTERACTIVE: Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
- SYSTEM: Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow

B.2.2 TriggerServer Properties

Open the TriggerServer Properties window by selecting *MMC -> Component Services -> Computers -> My Computer -> DCOM Config -> Trigger Server -> Properties*.

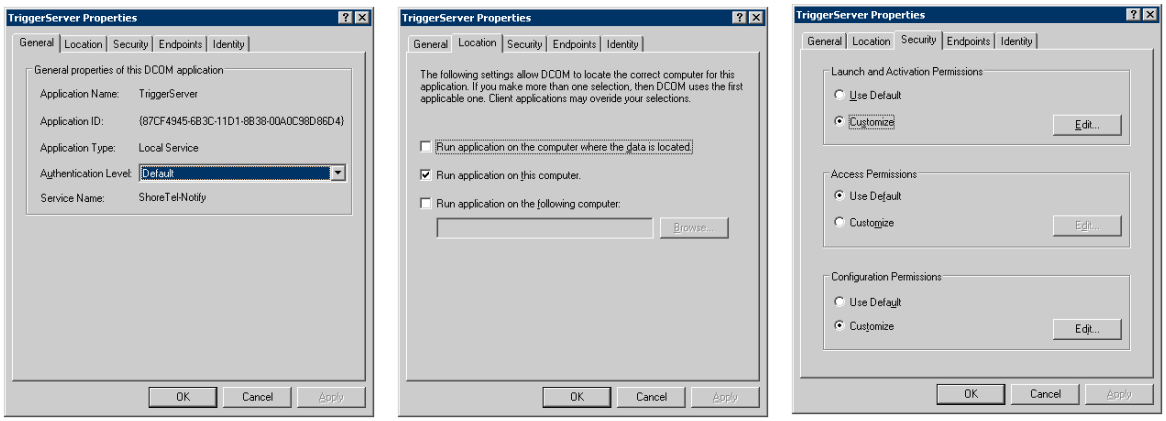

Figure B-5 TriggerServer Properties window – General, Location, and Security panels

Step 1 Open the **General** panel (Figure B-5).

Set **Authentication level** to ***Default***.

Step 2 Open the **Location** panel (Figure B-5).

Select ***Run application on this computer***.

Step 3 Open the **Security** panel (Figure B-5).

Step a Click ***Edit*** in the **Launch and Activation Permissions** section.

Select the following permissions, as shown in Figure B-6.

- Administrators: Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow

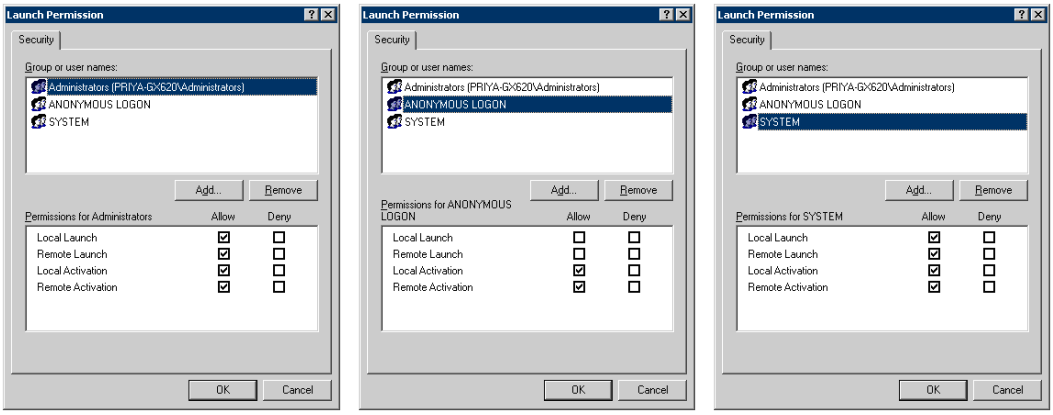

Figure B-6 Launch Permission window (TriggerServer)

- ANONYMOUS LOGON: Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow
- SYSTEM: Local Launch – allow; Remote Launch – allow
  Local Activation – allow; Remote Activation – allow

  Return to the **TriggerServer Properties: Security** panel by clicking *OK*.

Step b Click *Edit* in the **Configuration Permissions** section.

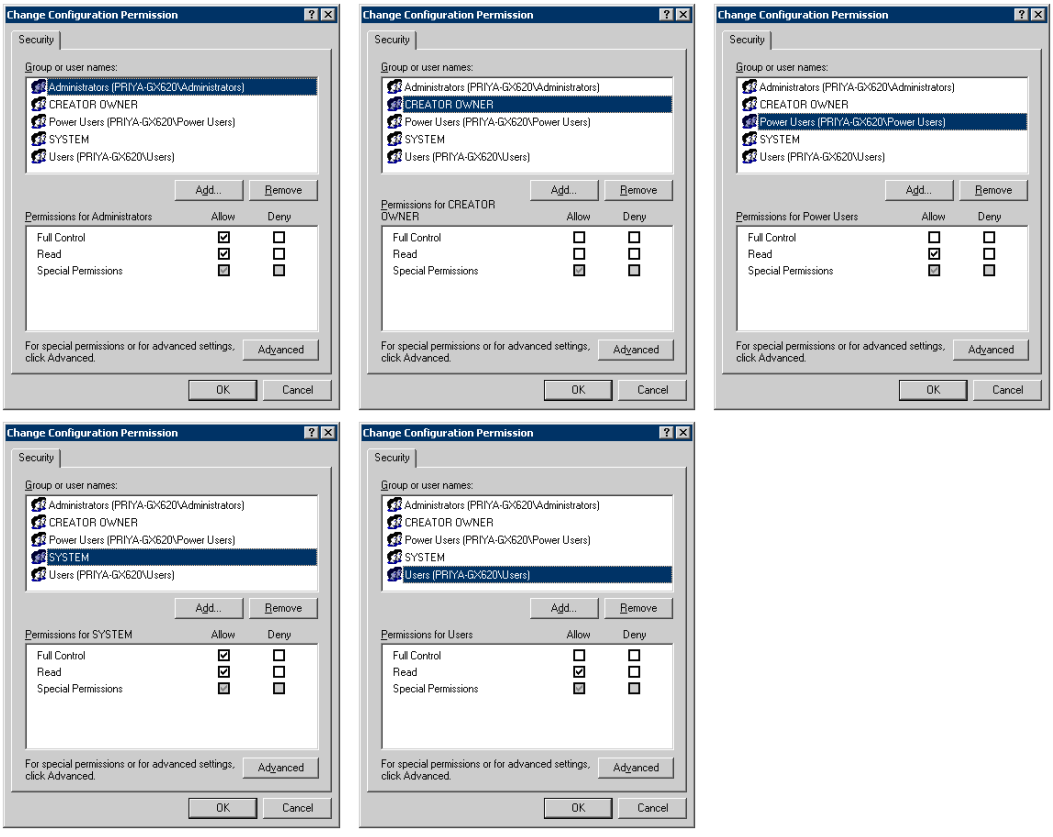

Figure B-7 Change Configuration Permission panel (TriggerServer)

Select the following permissions, as shown in Figure B-7:

- Administrators: Full Control – allow; Read – allow

- SYSTEM GROUP: Full Control – allow; Read – allow
- CREATOR OWNER: Full Control – no selection; Read – no selection
- other Users: Full Control – no selection; Read – allow

Return to the **TriggerServer Properties** window by clicking *OK*.

Step 4 Open the Identity panel (Figure B-8).

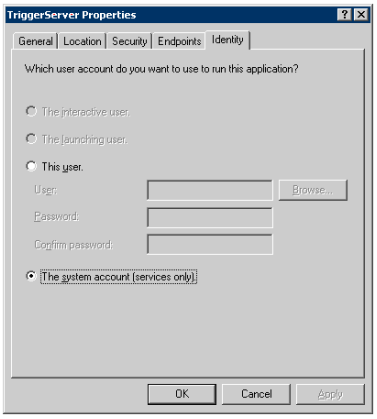

Figure B-8 TriggerServer Properties window – Identity panel

Select *The system account (services only)*.

B.2.3 Kadota Utilities Properties

Open the **KadotaUtil Properties** window by selecting *MMC -> Component Services -> Computers -> My Computer -> DCOM Config -> KadotaUtil*.

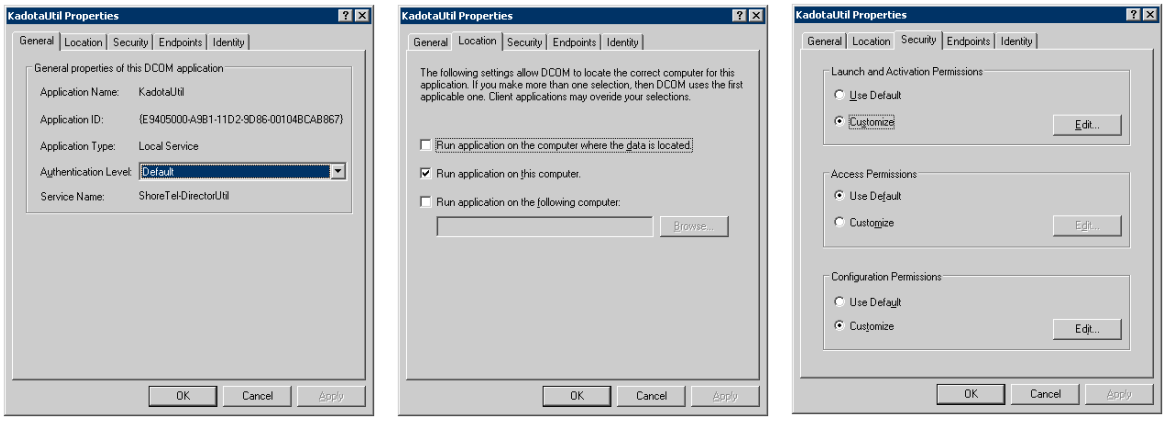

Figure B-9 Kadota Utility window – General, Location, and Security panels

Step 1 Open the **General** panel (Figure B-9).

Set **Authentication level** to *Default*.

Step 2 Open the **Location** panel. (Figure B-9).

Select *Run application on this computer*.

Step 3 Open the **Security** panel. (Figure B-9).

Step a Click *Edit* in the **Launch and Activation Permissions** section.

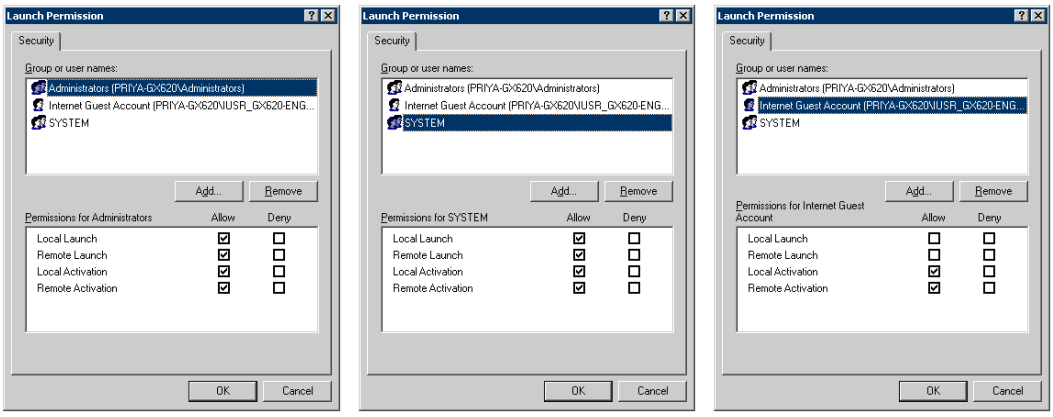

Figure B-10 Launch Permission panel (Kadota Utility)

Select the following permissions, as shown in Figure B-10.

- Administrators: Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
- Internal Guest Account: Local Launch – allow; Remote Launch – allow Local Activation – allow; Remote Activation – allow
- SYSTEM: Local Launch – no selection; Remote Launch – no selection Local Activation – allow; Remote Activation – allow.

Return to the **KadotaUtil Properties: Security** window by clicking *OK*.

Step b Click *Edit* in the **Configuration Permissions** section.

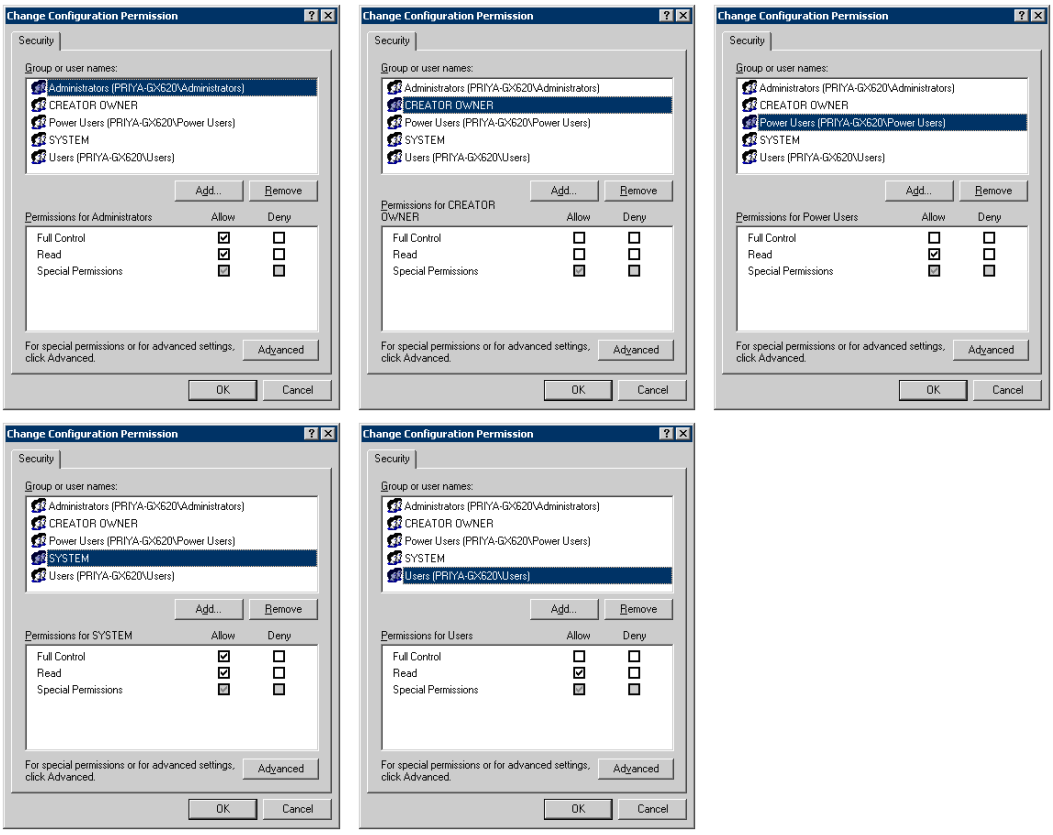

Figure B-11 Change Configuration Permission window (Kadota Utility)

Select the following permissions, as shown in Figure B-11.

- Administrators group: Full Control – allow; Read – allow
- CREATOR OWNER: Full Control – no selection; Read – no selection
- SYSTEM GROUP: Full Control – allow; Read – allow
- other User Groups: Full Control – no selection; Read – allow

Return to the KadotaUtil Properties window by clicking ***OK***.

Step 4 Open the Identity panel. (Figure B-12).

Select ***The system account (services only)***.

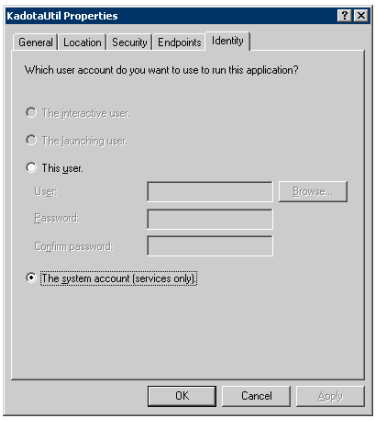

Figure B-12 Kadota Utility window – Identity panel

B.2.4 TMSManager2 Properties

Open the **TMSManager2 Properties** window by selecting *MMC -> Component Services -> Computers -> My Computer -> DCOM Config -> TMSManager2 -> Properties*.

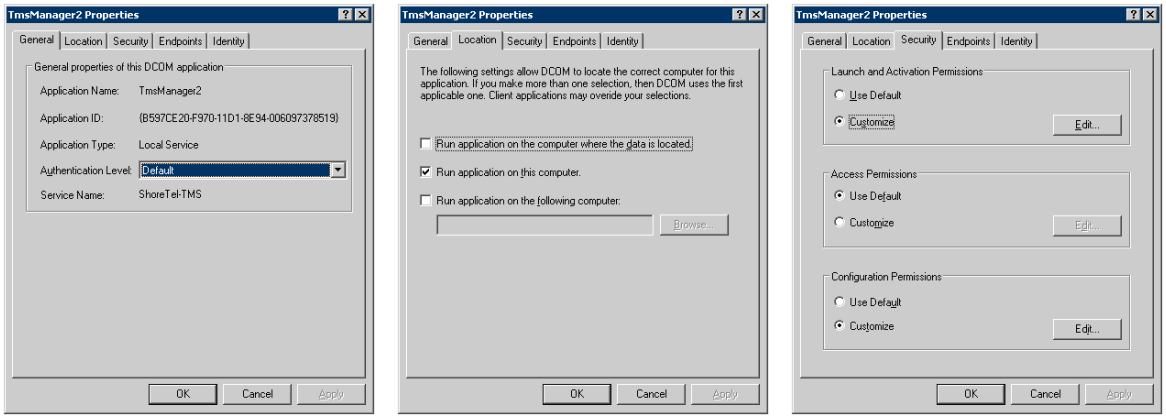

Figure B-13 TMSManager2 Properties window – General, Location, and Security panels

Step 1 Open the **General** panel (Figure B-13).

Set **Authentication level** to ***Default***.

Step 2 Open the **Location** panel (Figure B-13).

Select ***Run application on this computer***.

Step 3 Open the **Security** panel (Figure B-13).

Step a Click *Edit* in the **Launch and Activation Permissions** section.

Select the following permissions, as shown in Figure B-14.

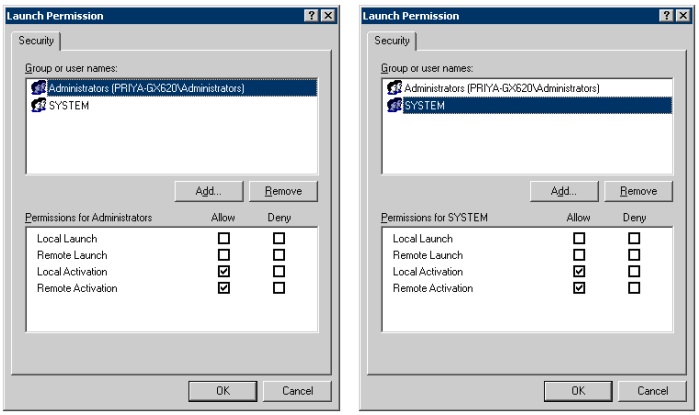

Figure B-14 Launch Permission window (TMSManager2 Properties)

- Administrators: Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow
- SYSTEM: Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow

Return to the TMSManager2 Properties window by clicking **OK**.

Step b Click *Edit* in the **Configuration Permissions** section.

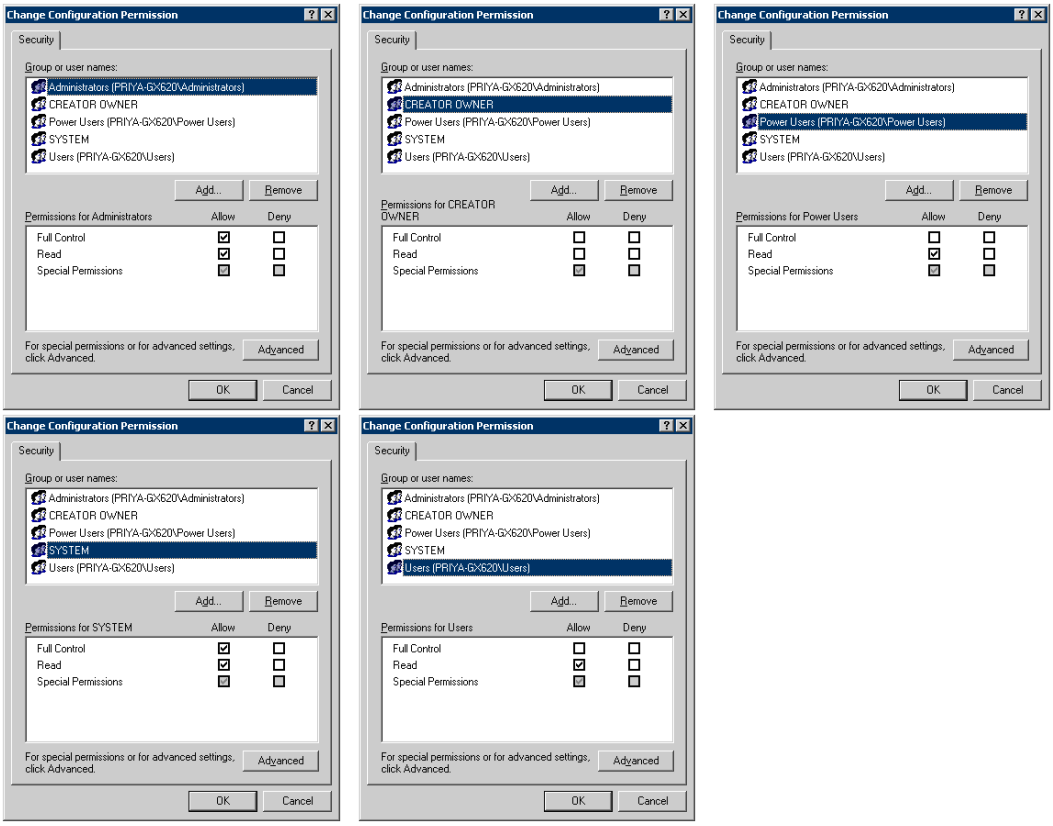

Figure B-15 Change Configuration Permission window (TMSManager2 Properties)

Select the following permissions, as shown in Figure B-15.

- Administrators: Full Control – allow; Read – allow
- CREATOR OWNER: Full Control – no selection; Read – no selection
- SYSTEM GROUP: Full Control – allow; Read – allow
- other Users: Full Control – no selection; Read – allow

Return to the TMSManager2 Properties window by clicking **OK**.

Step 4 Open the Identity panel (Figure B-16).

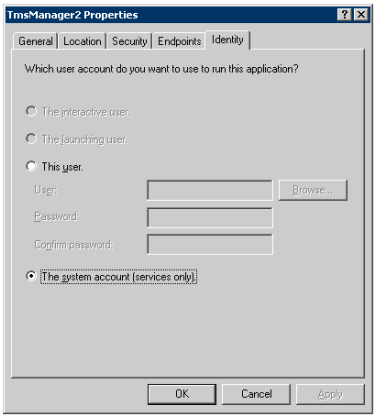

Figure B-16 TMSManager2 Properties panel – Identity

Select *The system account (services only)*

B.2.5 ZinManager Properties

Open the **ZinManager Properties** window by selecting *MMC -> Component Services -> computers -> My Computer -> DCOM Config -> ZinManager -> Properties.*

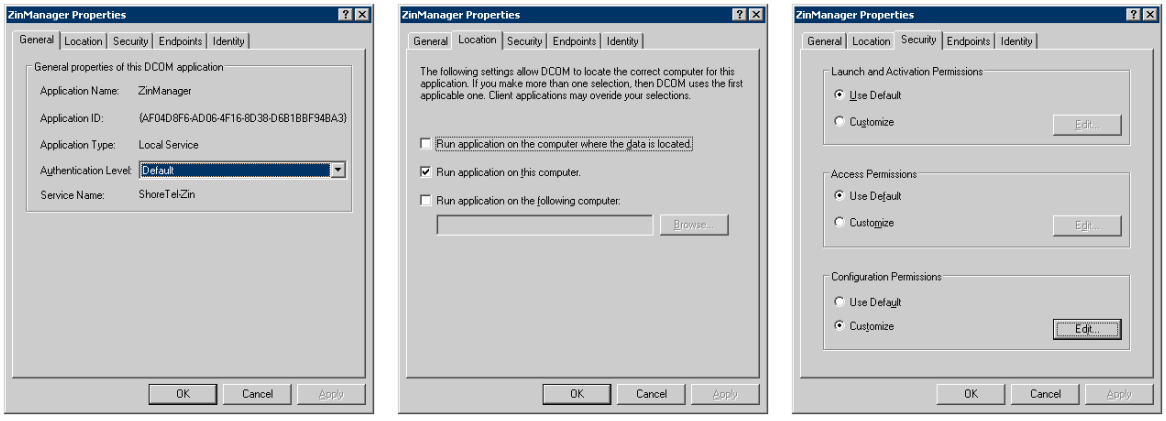

Figure B-17 ZinManager Properties panels – General, Location, and Security

Step 1 Open the **General** panel (Figure B-17).

Set **Authentication level** to *Default*.

Step 2 Open the **Location** panel (Figure B-17).

Select *Run application on this computer.*

Step 3 Open the **Security** panel (Figure B-17).

Step a Click ***Edit*** in the **Launch and Activation Permissions** section.

Select the following permissions, as shown in Figure B-18.

- Administrators: Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow
- SYSTEM: Local Launch – no selection; Remote Launch – no selection; Local Activation – allow; Remote Activation – allow

Return to the ZinManager Properties window by clicking **OK**.

Step b Click ***Edit*** in the **Configuration Permissions** section. Select the following permissions, as shown in Figure B-18.

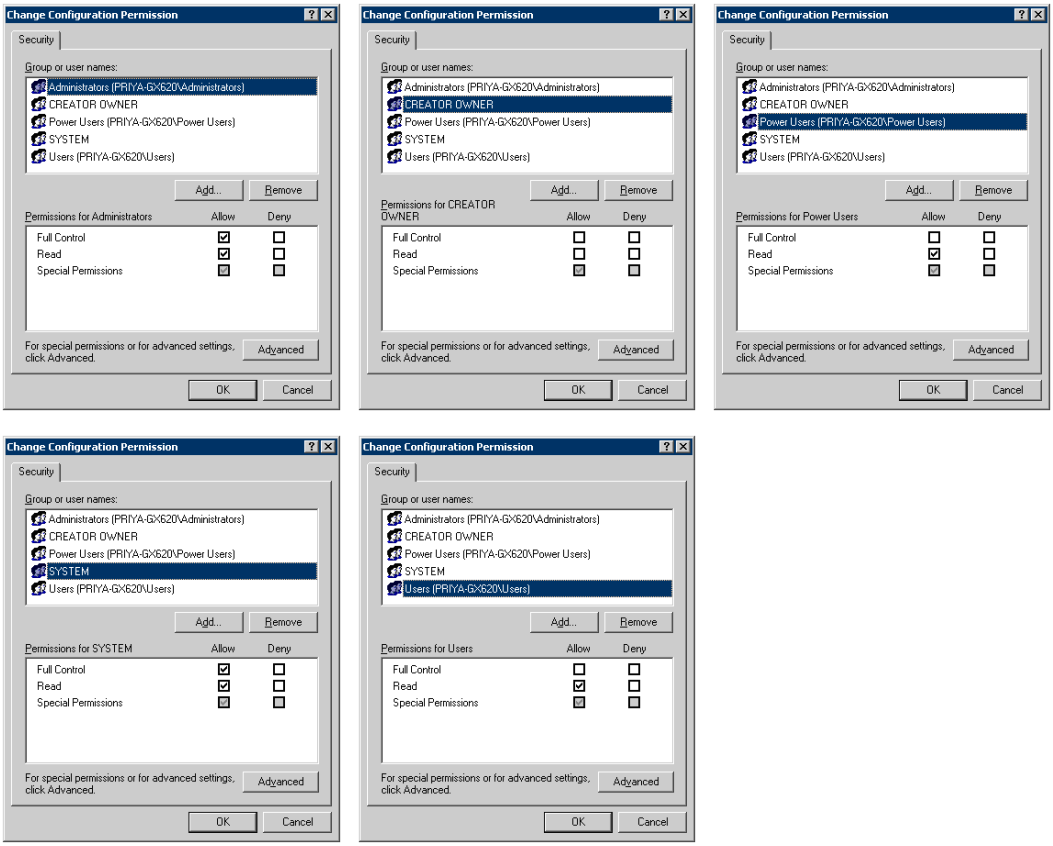

Figure B-18 Change Configuration Permission window (ZinManager)

- Administrators: Full Control – allow; Read – allow
- CREATOR OWNER: Full Control – no selection; Read – no selection
- SYSTEM: Full Control – allow; Read – allow

Return to the ZinManager Properties window by clicking **OK**.

Step 4 Open the Identity panel (Figure B-19).

Select ***The system account (services only)***.

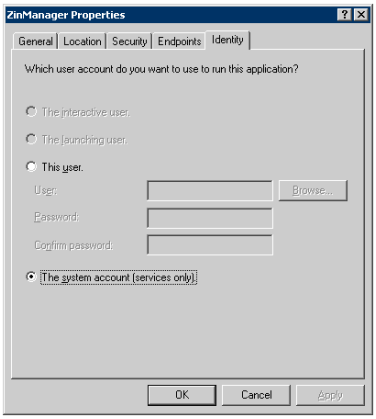

Figure B-19 ZinManager Properties panels – Identity

CHAPTER C

ShoreGear Switches

This appendix describes the ShoreGear voice switches. Switch model numbers are located on the rear panel, as shown in Figure C-1.

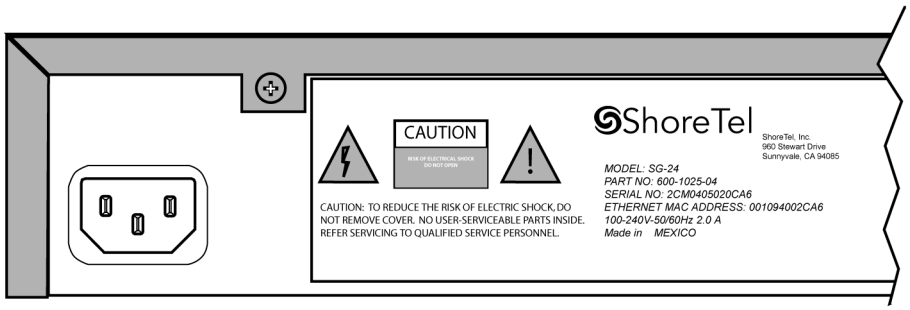
CAUTION
ShoreTel
ShoreTel, Inc.
960 Stewart Drive
Sunnyvale, CA 94085
CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE COVER. NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.
MODEL: SG-24
PART NO: 600-1025-04
SERIAL NO: 2CM0405020CA6
ETHERNET MAC ADDRESS: 001094002CA6
100-240V-50/60Hz 2.0 A
Made in MEXICO

Figure C-1 Switch Model Number Label

C.1 Switch Models

ShoreGear models are classified into three switch families, based on chassis type:

- 1-U Half Width Switches
- 1-U Full Width Switches
- IPBX Switches

The following is a brief description of each switch family.

C.1.1 ShoreGear 1-U Half Width Voice Switches

The ShoreGear 1-U Half Width Switch family is the most recent ShoreGear switch design. 1-U Half Width have a smaller footprint, use less power, and have lower heat dissipation requirements than earlier ShoreGear switches. These switches offer higher granularity in the number of IP users supported, allowing customers to precisely program the switch to satisfy their requirements.

The switches can be stacked or mounted in a standard 19-inch rack. Rack mounting 1-U Half Width Switches requires the ShoreTel Dual Tray. One or two switches are inserted into the Dual Tray, which is then mounted into the 19-inch rack. Two switches are mounted side by side Rack mounting the switches require the ShoreTel Dual Tray

ShoreGear 1-U Half Width Voice Switch models include:

- ShoreGear 30 (SG 30)
- ShoreGear 30BRI (SG 30BRI)
- ShoreGear 50 (SG 50)
- ShoreGear 90 (SG 90)

- ShoreGear 90BRI (SG 90BRI)
- ShoreGear 220T1 (SG 220T1)
- ShoreGear 220T1A (SG 220T1A)
- ShoreGear T1k (SG T1k)
- ShoreGear 220E1 (SG 220E1)
- ShoreGear E1k (SG E1k)

C.1.2 ShoreGear Voicemail Model Voice Switches

Voicemail Model Switches are ShoreGear switches that provide voicemail services and access to auto attendant menus for extensions hosted by the switch. Voicemail Model (V Model) switches provide local access to voicemail while being controlled by a Distributed server at a different location.

The switches can be stacked or mounted in a standard 19-inch rack. Rack mounting 1-U Half Width Switches requires the ShoreTel Dual Tray. One or two switches are inserted into the Dual Tray, which is then mounted into the 19-inch rack. Two switches are mounted side by side Rack mounting the switches require the ShoreTel Dual Tray

ShoreGear V Model Switch models include:

- ShoreGear 90V (SG 90V)
- ShoreGear 50V (SG 50V)
- ShoreGear 90BRIV (SG 90BRIV)

C.1.2.1 Capacity

Number of V Model switches allowed per system

A ShoreTel system supports a maximum of 100 V Model Switches. There are no restrictions concerning the allocation of switches among the sites defined by the system.

Simultaneous Voicemail Calls per V Model switches

Voicemail Model Switches support the following number of simultaneous voicemail calls.

- SG50V – Maximum of 5 Voicemail calls per switch
  - G711 calls: 5
  - G729 calls: 2
- SG50V – Maximum of 9 Voicemail calls per switch
  - G711 calls: 9
  - G729 calls: 4
- SG50V – Maximum of 9 Voicemail calls per switch
  - G711 calls: 9
  - G729 calls: 4

Call Load

Voicemail Model Switches call load capacity is as follows:

- 5400 BHCC when supporting 90 MGCP IP Phones or 90 SIP Trunks
- 3600 BHCC when supporting 90 SIP IP Phones or 90 SIP Trunks

Compact Flash Memory

Voicemail Model switches store voicemail and Auto Attendant files on compact flash. Flash card capacity for V Model Switches is:

- SG50V: 1 Gb
- SG90V: 2 Gb
- SG90BRIV: 2 Gb

Media Support

Voicemail Model Switches support the following media streams:

- G711
  - Music on Hold (MOH): 15 calls
  - Backup Auto Attendant (BAA): 50 calls
- G729
  - Music on Hold (MOH): none
  - Backup Auto Attendant (BAA): none

SIP support

Voicemail Model Switches support the following SIP media streams:

- G711 Ringback tone (Hunt Groups and Work Group calls): 50 media streams
- G729 Ringback tone (Hunt Groups and Work Group calls): no support

Restart & Reboot Time

V Model switches reboots require up to 4 minutes to complete

C.1.3 ShoreGear 1-U Full Width Voice Switches

The ShoreGear 1-U Full Width Switch family includes three models that support analog, IP, SIP, T1, and E1 voice data streams. Full width switch models can be stacked or mounted directly into a standard 19-inch equipment rack. These switches are all 1 RU and have an RJ21X connector for connection to analog phones and trunks. They also feature redundant Ethernet LAN connections for greater availability and reliability.

ShoreGear 1-U Full Width Voice Switch models include:

- ShoreGear 120 (SG 120) – also referred to as ShoreGear 120/24 (SG 120/24)
- ShoreGear 60 (SG 60) – also referred to as ShoreGear 60/12 (SG 60/12)
- ShoreGear 40 (SG 48) – also referred to as ShoreGear 40/8 (SG 40/8)
- ShoreGear T1 (SG T1)
- ShoreGear E1 (SG E1)
- ShoreGear 24A (SG 24A)

C.1.4 ShoreGear IPBX Voice Switches

The ShoreGear IPBX Switch family is the earliest ShoreGear switch design. Although ShoreTel no long markets IPBX switches, existing switches are supported and can be used in a ShoreTel network configuration. IPBX switches are full width and varying heights, depending on the switch model.

ShoreGear IPBX Voice Switch models include:

- ShoreGear 24 (IPBX 24) Voice Switch (2 RU)
- ShoreGear T1 (IPBX T1) Voice Switch (1.5 RU)
- ShoreGear E1 (IPBX E1) Voice Switch (1.5 RU)

C.2 Specifications – SG 1-U Half-Width Switches

C.2.1 ShoreGear 90 Voice Switch

The following sections describe ShoreGear 90 resource capacity, LED behavior, and connectors. The ShoreGear 90 is not supported in installations outside the U.S. and Canada. Figure C-2 displays the ShoreGear 90 front plate.

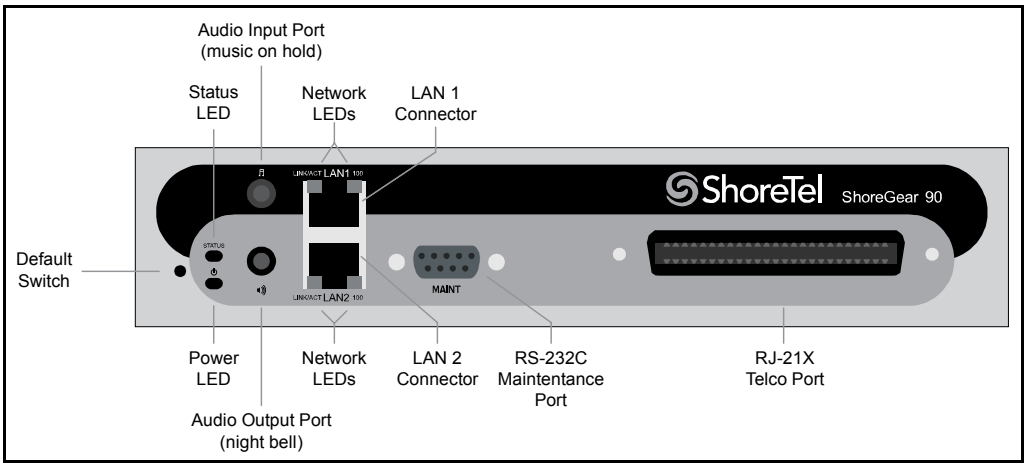

Figure C-2 ShoreGear 90 Front Plate

C.2.1.1 Switch Capacity

- **Analog Circuit Resources**
  - — ***Ports 1-8:*** Eight Loop Start Trunks
  - — ***Ports 9-12:*** Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
- **Make Me Conference Resources:** 12 ports
  - — ***Ports 1-12***
- **Maximum IP Phone Resources:** 90 devices
  - — ***Analog Port Reallocation:*** 60
  - — ***Built-in Resources:*** 30

C.2.1.2 LED Descriptions

Power LED

The ShoreGear 90 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing:**

- — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
- — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
- — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
- — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
- — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 90 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing)***, the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M:**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 90 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off**: No ports are assigned.

C.2.1.3 ShoreGear 90 Connectors

The ShoreGear 90 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
  - — ***Backup Operator:*** Extension Port 12

ShoreGear 90 RJ-21X Telephone and Trunk Connector

Table C-1 lists the RJ-21X Ring and Tip pin numbers for the SG 90

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5	Trunk	9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6	Trunk	11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7	Trunk	13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8	Trunk	15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange

Table C-1 ShoreGear 90 RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-1 ShoreGear 90 RJ-21X Telephone and Trunk Connector Pins

C.2.2 ShoreGear 90BRI Voice Switch

The following sections describe ShoreGear 90BRI resource capacity, LED behavior, and connectors. Figure C-3 displays the ShoreGear 90BRI front plate.

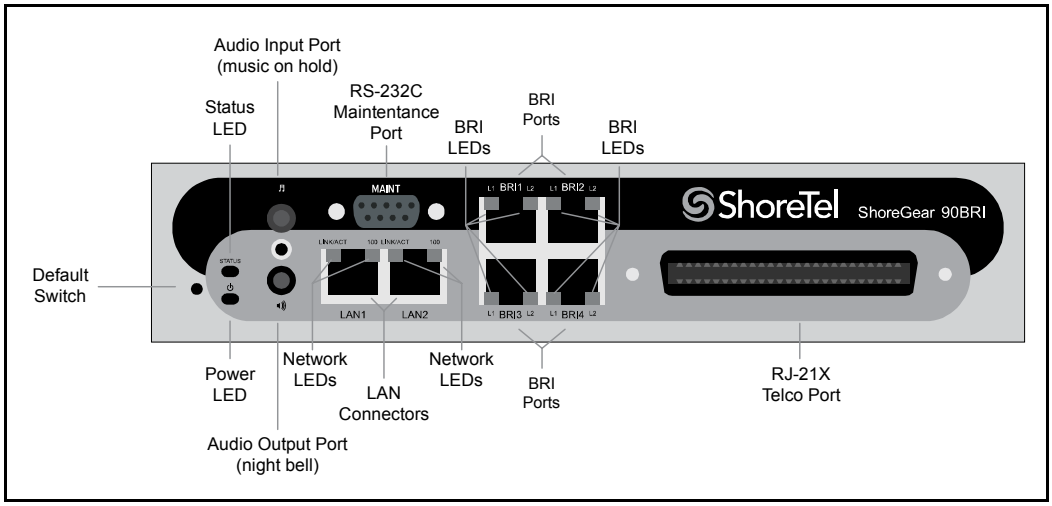

Figure C-3 ShoreGear 90BRI Front Plate

C.2.2.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 9-12:* Extensions
- Digital Circuit Resources
  - — *Four BRI Spans, each comprising two channels:* Eight channels maximum
- Make Me Conference Resource: None
- Maximum IP Phone Resources: 90 devices
  - — *Analog Port Reallocation:* 20
  - — *Digital Channel Reallocation:* 40
  - — *Built-in Resources:* 30

C.2.2.2 LED Descriptions

Power LED

The ShoreGear 90BRI has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 90BRI network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — When flashing, network activity is detected.
  - — When on (not flashing), the switch is connected to an Ethernet network.
  - — When off, the switch cannot detect an Ethernet network.

This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 90BRI has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady***, no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow*** (1 sec. on/off), the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- — **LED 1: Off, LED 2 Off –** Port not configured in Director
- — **LED 1: Yellow, LED 2 Off –** Port inactive or not connected
- — **LED 1: Off, LED 2 Off –** Layer 1 active. Layer 2 not established
- — **LED 1: Off, LED 2 Green –** Layer 1 active. Layer 2 active.
- — **LED 1: Off, LED 2 Green flashing –** Call in progress (Layer 1, Layer 2, and Layer 3 active).

C.2.2.3 ShoreGear 90BRI Connectors

The ShoreGear 90BRI voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
- 4 RJ-45 T1 telco port

ShoreGear 90BRI RJ-21X Telephone and Trunk Connector

Table C-2 lists the RJ-21X Ring and Tip pin numbers for the SG 90BRI

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–		3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-2 ShoreGear 90BRI RJ-21X Telephone and Trunk Connector Pins

C.2.3 ShoreGear 50 Voice Switch

The following sections describe ShoreGear 50 rresource capacity, LED behavior, and connectors. The ShoreGear 50 is not supported in installations outside the U.S. and Canada. Figure C-4 displays the ShoreGear 50 front plate.

C.2.3.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 1-4:* Four Loop Start Trunks
  - — *Ports 11-12:* Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - — *Power Failure Transfer Unit:* Trunk Port 1 to Extension Port 12
- Make Me Conference Resources: six ports
  - — *Ports 1-4, 11-12*

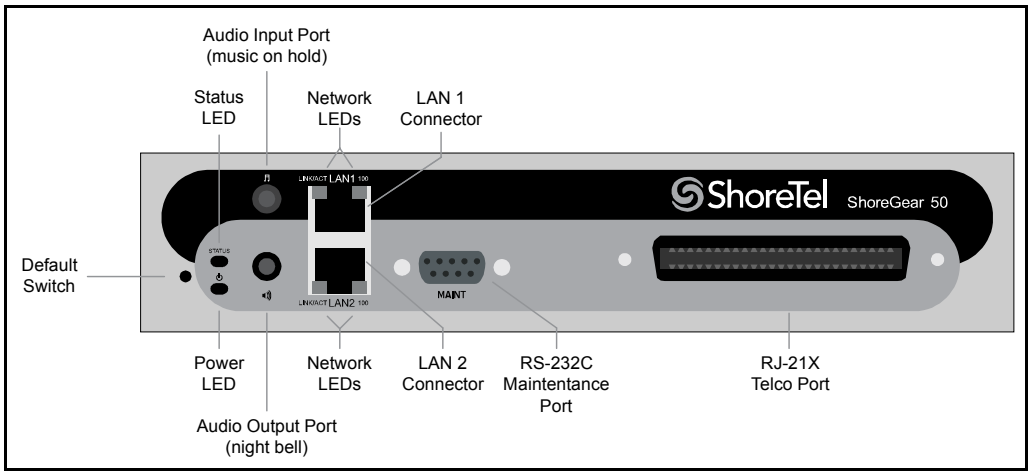

Figure C-4 ShoreGear 50 Front Plate

- **Maximum IP Phone Resources:** 50 devices
  - — ***Analog Port Reallocation:*** 30
  - — ***Built-in Resources:*** 20

C.2.3.2 LED Descriptions

Power LED

The ShoreGear 50 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If

the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 50 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 50 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady***, no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow***, the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

C.2.3.3 ShoreGear 50 Connectors

The ShoreGear 50 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface

- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
  — ***Backup Operator:*** Extension Port 12

ShoreGear 50 RJ-21X Telephone and Trunk Connector

Table C-3 lists the RJ-21X Ring and Tip pin numbers for the SG 50

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-3 ShoreGear 50 RJ-21X Telephone and Trunk Connector Pins

C.2.4 ShoreGear 30 Voice Switch

The following sections describe ShoreGear 30 resource capacity, LED behavior, and connectors. The ShoreGear 30 is not supported in installations outside the U.S. and Canada. Figure C-5 displays the ShoreGear 30 front plate.

C.2.4.1 Switch Capacity

- Analog Circuit Resources

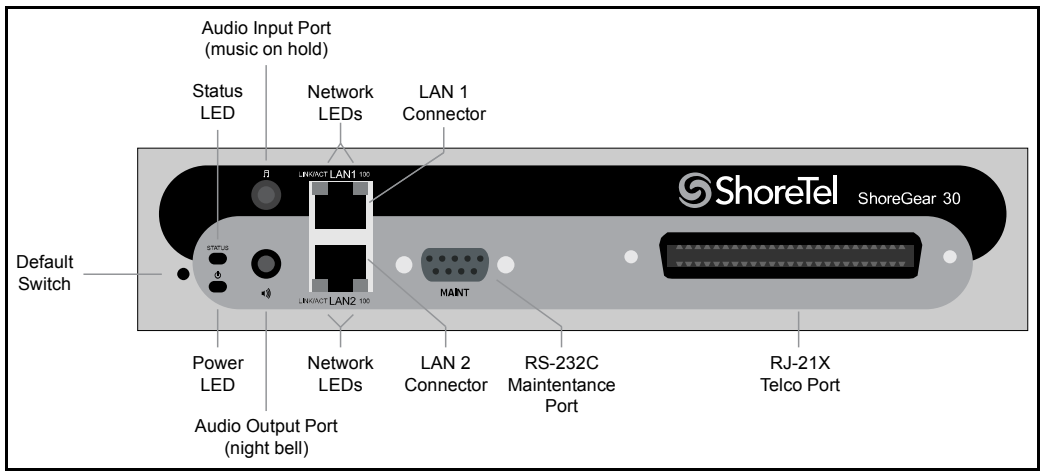

Figure C-5 ShoreGear 30 Front Plate

— ***Ports 1-2:*** Two Loop Start Trunks
— ***Ports 11-12:*** Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.

— ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12

- **Make Me Conference Resources:** none
- **Maximum IP Phone Resources:** none
  — ***Analog Port Reallocation:*** 20
  — ***Built-in Resources:*** 10

C.2.4.2 LED Descriptions

Power LED

The ShoreGear 30 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing:**
  — ***2 flashes—***The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  — ***3 flashes—***Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  — ***4 flashes—***The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  — ***5 flashes—***The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to

`/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.

— ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 30 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity**: When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - ***When flashing,*** network activity is detected.
  - ***When on (not flashing)***, the switch is connected to an Ethernet network.
  - ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**:
  - ***When green,*** the switch is connected to a 100BaseT network.
  - ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 30 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - ***When on steady,*** no ports are handling active calls.
  - ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off**: No ports are assigned.

C.2.4.3 ShoreGear 30 Connectors

The ShoreGear 30 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
  - — ***Backup Operator:*** Extension Port 12

ShoreGear 30 RJ-21X Telephone and Trunk Connector

Table C-4 lists the RJ-21X Ring and Tip pin numbers for the SG 30

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-4 ShoreGear 30 RJ-21X Telephone and Trunk Connector Pins

C.2.5 ShoreGear 30BRI Voice Switch

The following sections describe ShoreGear 30BRI resource capacity, LED behavior, and connectors. Figure C-6 displays the ShoreGear 30BRI front plate.

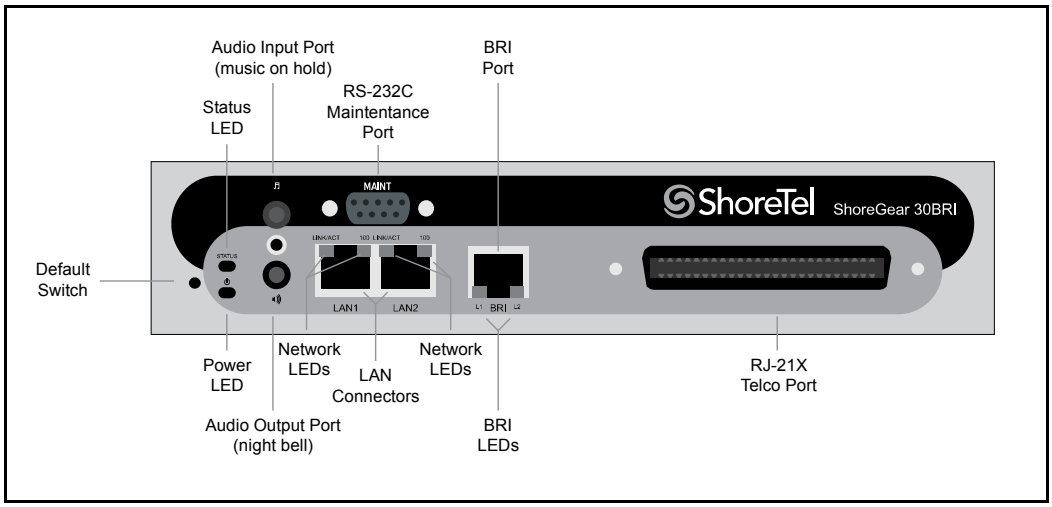

Figure C-6 ShoreGear 30BRI Front Plate

C.2.5.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 11-12:* Extensions
- Digital Circuit Resources
  - — *One BRI Span comprising two channels:* two channels maximum
- **Make Me Conference Resource:** None
- **Maximum IP Phone Resources:** 30 devices
  - — *Analog Port Reallocation:* 10
  - — *Digital Channel Reallocation:* 10
  - — *Built-in Resources:* 10

C.2.5.2 LED Descriptions

Power LED

The ShoreGear 30BRI has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.

— ***4 flashes—***The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.

— ***5 flashes—***The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.

— ***6 flashes—***Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 30BRI network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  — When flashing, network activity is detected.
  — When on (not flashing), the switch is connected to an Ethernet network.
  — When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

- **100M**
  — ***When green,*** the switch is connected to a 100BaseT network.
  — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 30BRI has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  — ***When on steady,*** no ports are handling active calls.
  — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call.

- **Status LED (Yellow)**

- *When on steady*, no ports are handling active calls and at least one port is out of service.
- *When flashing slow* (1 sec. on/off), the switch is not connected (or has lost connection) to a ShoreTel server.
- *When flashing fast* (100 msec on/off), at least one port is handling an active call and at least one port is out of service.

- **Off:** No ports are assigned.

BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- **LED 1: Off, LED 2 Off –** Port not configured in Director
- **LED 1: Yellow, LED 2 Off –** Port inactive or not connected
- **LED 1: Off, LED 2 Off –** Layer 1 active. Layer 2 not established
- **LED 1: Off, LED 2 Green –** Layer 1 active. Layer 2 active.
- **LED 1: Off, LED 2 Green flashing –** Call in progress (Layer 1, Layer 2, and Layer 3 active).

C.2.5.3 ShoreGear 30BRI Connectors

The ShoreGear 30BRI voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
- 4 RJ-45 T1 telco port

ShoreGear 30BRI RJ-21X Telephone and Trunk Connector

Table C-5 lists the RJ-21X Ring and Tip pin numbers for the SG 30BRI

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–		3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green

Table C-5 ShoreGear 30BRI RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-5 ShoreGear 30BRI RJ-21X Telephone and Trunk Connector Pins

C.2.6 ShoreGear 220T1 Voice Switch

The following sections describe ShoreGear 220T1 resource capacity, LED behavior, and connectors. The ShoreGear 220T1 is not supported in installations outside the U.S. and Canada. Figure C-7 displays the ShoreGear 220T1 front plate.

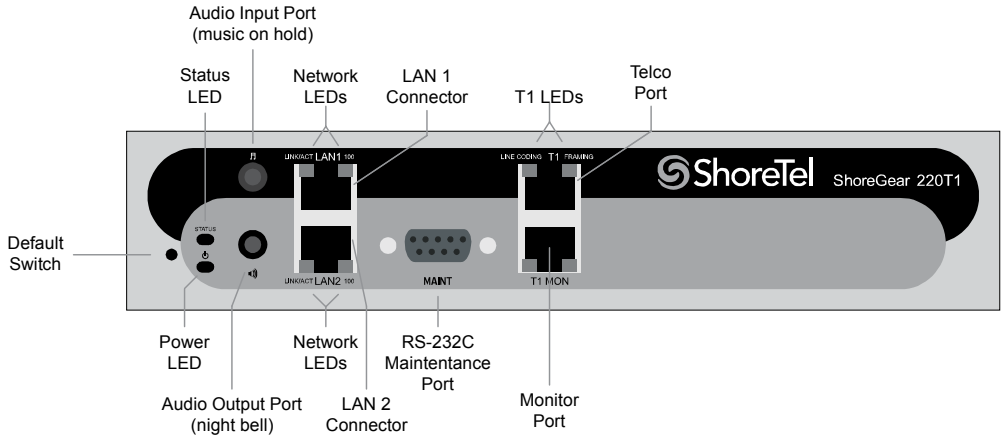

Figure C-7 ShoreGear 220T1 Front Plate

C.2.6.1 Switch Capacity

- **Digital Circuit Resources:** 24 channels maximum
  - — *One T1 circuit, 24 channels per circuit:* 24 channels maximum
- **Make Me Conference Resource:** None
- **Maximum IP Phone Resources:** 220
  - — *Digital Channel Reallocation:* 120
  - — *Built-in Resources:* 100

C.2.6.2 LED Descriptions

Power LED

The ShoreGear 220T1 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 220T1 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

TheShoreGear 220T1 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are being received at one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** a series of frame-bit errors (>1 per 1000) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.

C.2.6.3 ShoreGear 220T1 Connectors

The ShoreGear 220T1 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

C.2.7 ShoreGear 220T1A Voice Switch

The following sections describe ShoreGear 220T1A resource capacity, LED behavior, and connectors. The ShoreGear 220T1A is not supported in installations outside the U.S. and Canada. Figure C-8 displays the ShoreGear 220T1A front plate.

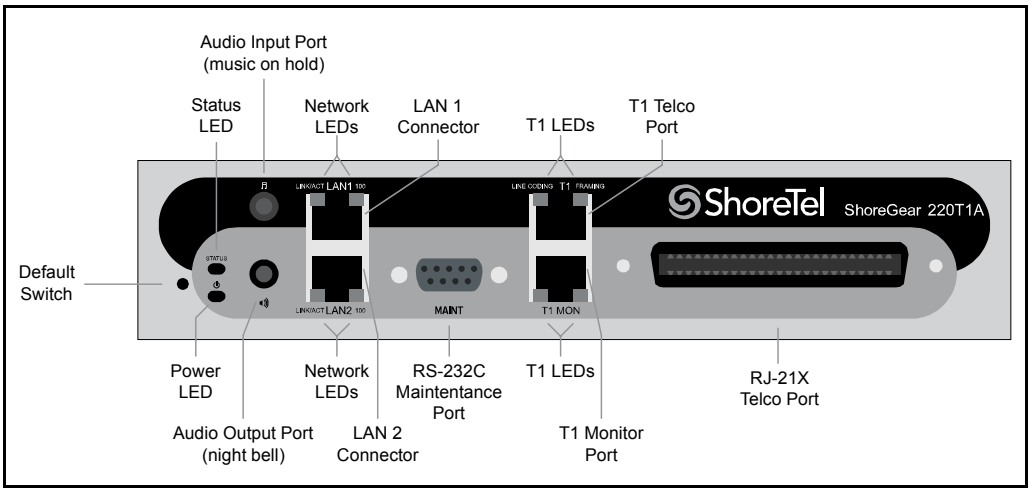

Figure C-8 ShoreGear 220T1A Front Plate

C.2.7.1 Switch Capacity

- **Analog Circuit Resources**
  - — *Ports 1-2:* Two Loop Start Trunks
  - — *Ports 9-12:* Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - — *Power Failure Transfer Unit:* Trunk Port 1 to Extension Port 12
- **Digital Circuit Resources**: 24 channels maximum
  - — *One T1 circuit, 24 channels per circuit*
- **Make Me Conference Resource**: Six ports
  - — *Ports 1-2, 9-12*
- **Maximum IP Phone Resources**: 220 devices
  - — *Analog Channel Reallocation:* 30
  - — *Digital Channel Reallocation:* 120
  - — *Built-in Resources:* 70

C.2.7.2 LED Descriptions

Power LED

The ShoreGear 220T1A has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 220T1A network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 220T1A has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow*** (1 sec. on/off), the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are received at one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits.
  - — ***When flashing slow yellow,*** a small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** a series of frame-bit errors (> 1 per 1000) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.

C.2.7.3 ShoreGear 220T1A Connectors

The ShoreGear 220T1A voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

ShoreGear 220T1A RJ-21X Telephone and Trunk Connector

Table C-6 lists the RJ-21X Ring and Tip pin numbers for the SG 220T1AI

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-6 ShoreGear 220T1A RJ-21X Telephone and Trunk Connector Pins

C.2.8 ShoreGear-220E1 Voice Switch

The following sections describe ShoreGear-220E1 resource capacity, LED behavior, and connectors. Figure C-9 displays the ShoreGear-220E1 front plate.

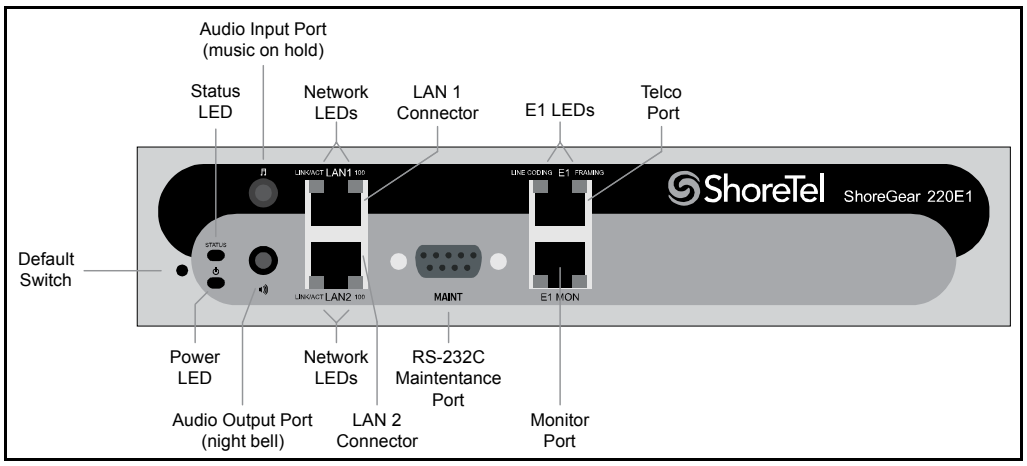

Figure C-9 ShoreGear-220E1 Front Plate

C.2.8.1 Switch Capacity

- **Digital Circuit Resources:** 30 channels maximum
  - — *One E1 circuit, 30 channels per circuit*
- **Make Me Conference Resource:** none
- **Maximum IP Phone Resources:** 220
  - — *Digital Channel Reallocation:* 150
  - — *Built-in Resources:* 70

C.2.8.2 LED Descriptions

Power LED

The ShoreGear-220E1 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67,

set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.

— ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear-220E1 network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on*** (not flashing), the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear-220E1 has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are being received at one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits.
  - — ***When flashing slow yellow,*** a small number of frame-bit errors ($10e^{-6}$) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** a series of frame-bit errors ($10e^{-3}$) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.

C.2.8.3 ShoreGear-220E1 Connectors

The ShoreGear-220E1 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

C.2.9 ShoreGear T1k Voice Switch

The following sections describe ShoreGear T1k resource capacity, LED behavior, and connectors. The ShoreGear T1k is not supported in installations outside the U.S. and Canada. Figure C-10 displays the ShoreGear T1k front plate.

C.2.9.1 Switch Capacity

- **Digital Circuit Resources:** 24 channels maximum
  - — ***One T1 circuit, 24 channels per circuit***
- **Make Me Conference Resource:** None
- **Maximum IP Phone Resources:** None

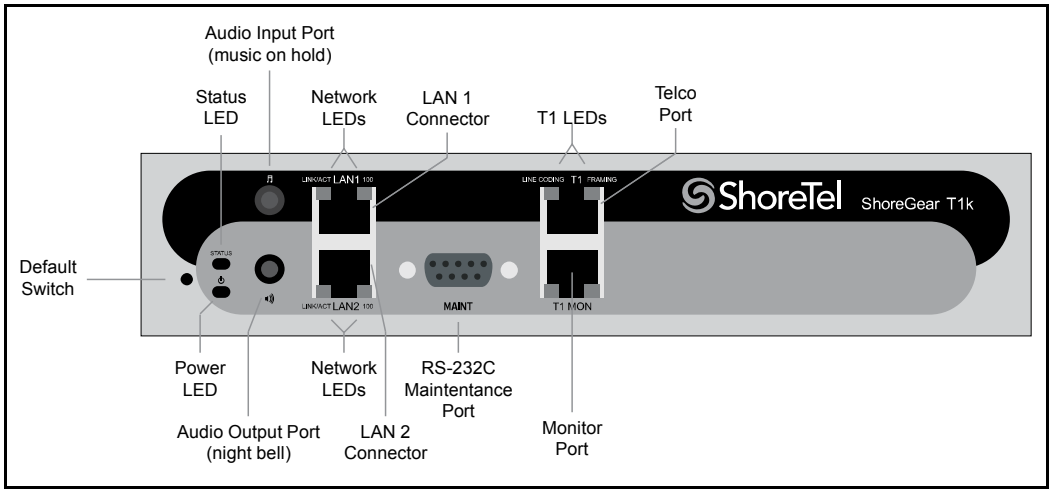

Figure C-10 ShoreGear T1k Front Plate

C.2.9.2 LED Descriptions

Power LED

The ShoreGear T1k has one power LED, which indicates the following:

- **On**: The switch is operating normally.
- **Off**: The switch has no power.
- **Flashing**
  - — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops

flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear T1k network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear T1k has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are being received at one second intervals.

— ***When red,*** a loss of signal (LOS) has occurred.
— ***When flashing red,*** loopback is active (local or CO).
— ***When off,*** the switch has no power.

- **Framing:** This LED indicates network framing status, as follows:
  — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  — ***When flashing fast yellow,*** a series of frame-bit errors (>1 per 1000) have occurred.
  — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  — ***When flashing red,*** loopback is active (local or CO).
  — ***When off,*** the switch has no power.

C.2.9.3 ShoreGear T1k Connectors

The ShoreGear T1k voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

C.2.10 ShoreGear E1k Voice Switch

The following sections describe ShoreGear E1k resource capacity, LED behavior, and connectors. The ShoreGear E1k is not supported in installations outside the U.S. and Canada. Figure C-10 displays the ShoreGear E1k front plate.

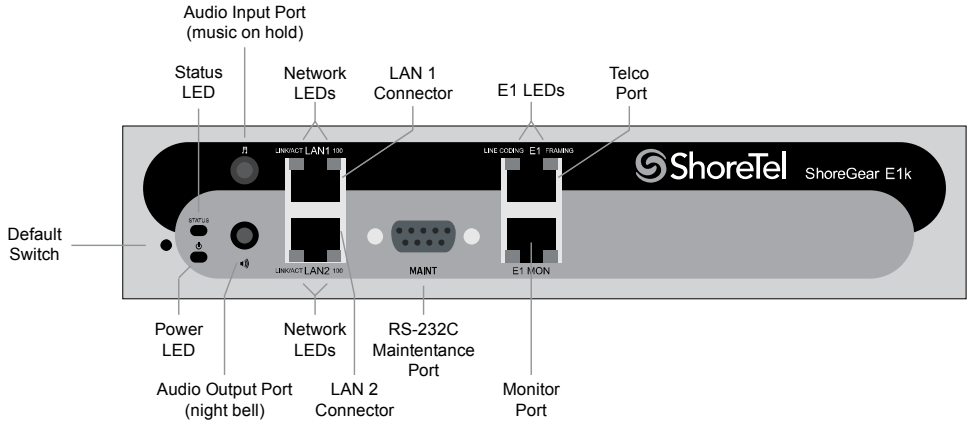

Figure C-11 ShoreGear E1k Front Plate

C.2.10.1 Switch Capacity

- **Digital Circuit Resources:** 30 channels maximum
  — ***One E1 circuit, 30 channels per circuit***
- **Make Me Conference Resource:** None

- **Maximum IP Phone Resources:** None

C.2.10.2 LED Descriptions

Power LED

The ShoreGear E1k has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes*—**Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear E1k network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear E1k has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are being received at one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits. A small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** a series of frame-bit errors (>1 per 1000) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.

C.2.10.3 ShoreGear E1k Connectors

The ShoreGear E1k voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

C.3 Specifications – SG Voice Model Switches

C.3.1 ShoreGear 90V Voice Switch

The following sections describe ShoreGear 90V resource capacity, LED behavior, and connectors. The ShoreGear 90V is not supported in installations outside the U.S. and Canada. Figure C-12 displays the ShoreGear 90V front plate.

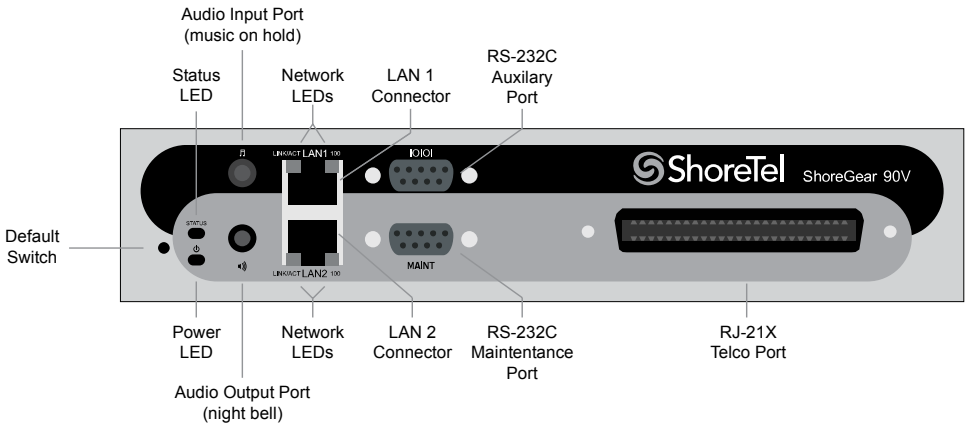

Figure C-12 ShoreGear 90V Front Plate

C.3.1.1 Switch Capacity

- **Analog Circuit Resources**
  - — ***Ports 1-8:*** Eight Loop Start Trunks
  - — ***Ports 9-12:*** Four Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
- **Make Me Conference Resources:** 12 ports
  - — ***Ports 1-12***
- **Maximum IP Phone Resources:** 90 devices
  - — ***Analog Port Reallocation:*** 60
  - — ***Built-in Resources:*** 30

C.3.1.2 LED Descriptions

Power LED

The ShoreGear 90V has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing:**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure. Replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.

- — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
- — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
- — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
- — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 90V network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing)***, the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M:**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 90V has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.

- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow,*** the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

C.3.1.3 ShoreGear 90V Connectors

The ShoreGear 90V voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
  - — ***Backup Operator:*** Extension Port 12

ShoreGear 90V RJ-21X Telephone and Trunk Connector

Table C-7 lists the RJ-21X Ring and Tip pin numbers for the ShoreGear 90V

		Ring		Tip	
Port	Type	Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
5	Trunk	9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
6	Trunk	11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
7	Trunk	13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
8	Trunk	15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate

Table C-7 ShoreGear 90V RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-7 ShoreGear 90V RJ-21X Telephone and Trunk Connector Pins

C.3.2 ShoreGear 90BRIV Voice Switch

The following sections describe ShoreGear 90BRIV resource capacity, LED behavior, and connectors. Figure C-13 displays the ShoreGear 90BRIV front plate.

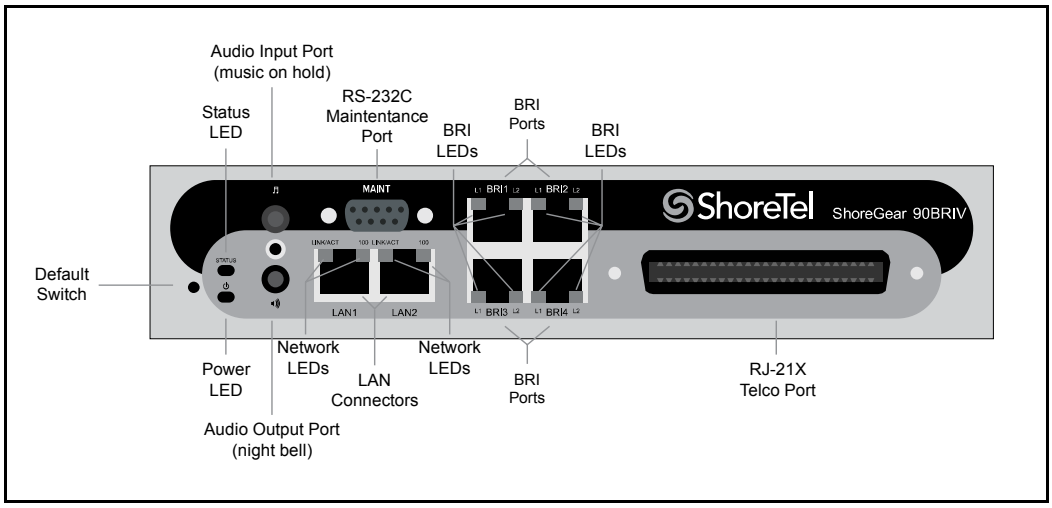

Figure C-13 ShoreGear 90BRIV Front Plate

C.3.2.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 9-12:* Extensions
- Digital Circuit Resources
  - — *Four BRI Spans, each comprising two channels:* Eight channels maximum
- **Make Me Conference Resource**: None
- **Maximum IP Phone Resources**: 90 devices
  - — *Analog Port Reallocation:* 20
  - — *Digital Channel Reallocation:* 40
  - — *Built-in Resources:* 30

C.3.2.2 LED Descriptions

Power LED

The ShoreGear 90BRIV has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes—***The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes—***Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes—***The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes—***The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — ***6 flashes—***Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 90BRIV network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — When flashing, network activity is detected.
  - — When on (not flashing), the switch is connected to an Ethernet network.
  - — When off, the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.

  - **100M**

  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 90BRIV has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady,*** no ports are handling active calls.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady***, no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow*** (1 sec. on/off), the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast*** (100 msec on/off), at least one port is handling an active call and at least one port is out of service.
- **Off**: No ports are assigned.

BRI LED

Each BRI connector has two LEDs to indicate port activity. The color and blink pattern of the LED indicate the port function:

- — **LED 1: Off, LED 2 Off –** Port not configured in Director
- — **LED 1: Yellow, LED 2 Off –** Port inactive or not connected
- — **LED 1: Off, LED 2 Off –** Layer 1 active. Layer 2 not established
- — **LED 1: Off, LED 2 Green –** Layer 1 active. Layer 2 active.
- — **LED 1: Off, LED 2 Green flashing –** Call in progress (Layer 1, Layer 2, and Layer 3 active).

C.3.2.3 ShoreGear 90BRIV Connectors

The ShoreGear 90BRIV voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
- 4 RJ-45 T1 telco port

ShoreGear 90BRIV RJ-21X Telephone and Trunk Connector

Table C-8 lists the RJ-21X Ring and Tip pin numbers for the SG 90BRIV

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
–		3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
–		5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue

Table C-8 ShoreGear 90BRIV RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-8 ShoreGear 90BRIV RJ-21X Telephone and Trunk Connector Pins

C.3.3 ShoreGear 50V Voice Switch

The following sections describe ShoreGear 50V rresource capacity, LED behavior, and connectors. The ShoreGear 50V is not supported in installations outside the U.S. and Canada. Figure C-14 displays the ShoreGear 50V front plate.

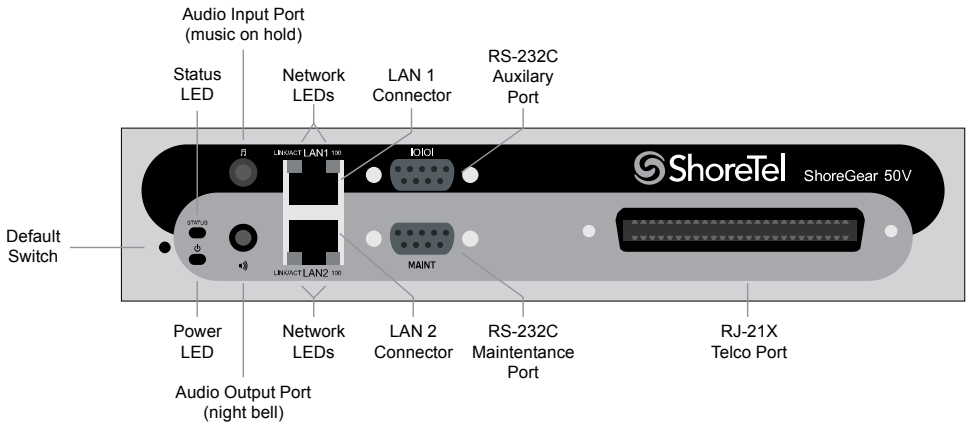

Figure C-14 ShoreGear 50V Front Plate

C.3.3.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 1-4:* Four Loop Start Trunks
  - — *Ports 11-12:* Two Extensions or DID Trunks. A single command configures all ports as either Extensions or DID trunks.
  - — *Power Failure Transfer Unit:* Trunk Port 1 to Extension Port 12
- **Make Me Conference Resources:** six ports
  - — *Ports 1-4, 11-12*
- **Maximum IP Phone Resources:** 50 devices
  - — *Analog Port Reallocation:* 30
  - — *Built-in Resources:* 20

C.3.3.2 LED Descriptions

Power LED

The ShoreGear 50V has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsk/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsk/vxworks`.
  - — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The ShoreGear 50V network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on (not flashing),*** the switch is connected to an Ethernet network.
  - — ***When off,*** the switch cannot detect an Ethernet network.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

Status LED

The ShoreGear 50V has one status LED to provide general information about the ports. The color and blink pattern of the LED indicate the port function:

- **Status LED (Green)**
  - — ***When on steady***, no ports are handling active calls.
  - — ***When flashing fast,*** at least one port is handling an active call.
- **Status LED (Yellow)**
  - — ***When on steady,*** no ports are handling active calls and at least one port is out of service.
  - — ***When flashing slow***, the switch is not connected (or has lost connection) to a ShoreTel server.
  - — ***When flashing fast,*** at least one port is handling an active call and at least one port is out of service.
- **Off:** No ports are assigned.

C.3.3.3 ShoreGear 50V Connectors

The ShoreGear 50V voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 1 to Extension Port 12
  - — ***Backup Operator:*** Extension Port 12

ShoreGear 50V RJ-21X Telephone and Trunk Connector

Table C-9 lists the RJ-21X Ring and Tip pin numbers for the SG 50V

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk	1	Blue/White	26	White/Blue
–		2	Orange/White	27	White/Orange
2	Trunk	3	Green/White	28	White/Green
–		4	Brown/White	29	White/Brown
3	Trunk	5	Slate/White	30	White/Slate
–		6	Blue/Red	31	Red/Blue
4	Trunk	7	Orange/Red	32	Red/Orange
–		8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
9	Extension - DID	17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
10	Extension - DID	19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
11	Extension - DID	21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
12	Extension - DID	23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-9 ShoreGear 50V RJ-21X Telephone and Trunk Connector Pins

C.4 Specification – SG 1U Full Width Switches

C.4.1 ShoreGear 120 Voice Switch

The following sections describe ShoreGear 120 resource capacity, LED behavior, and connectors. The ShoreGear 120 is not supported in installations outside the U.S. and Canada. Figure C-15 displays the ShoreGear 120 front plate.

The ShoreGear 120 is often referred to as the ShoreGear 120/24 (SG 120/24).

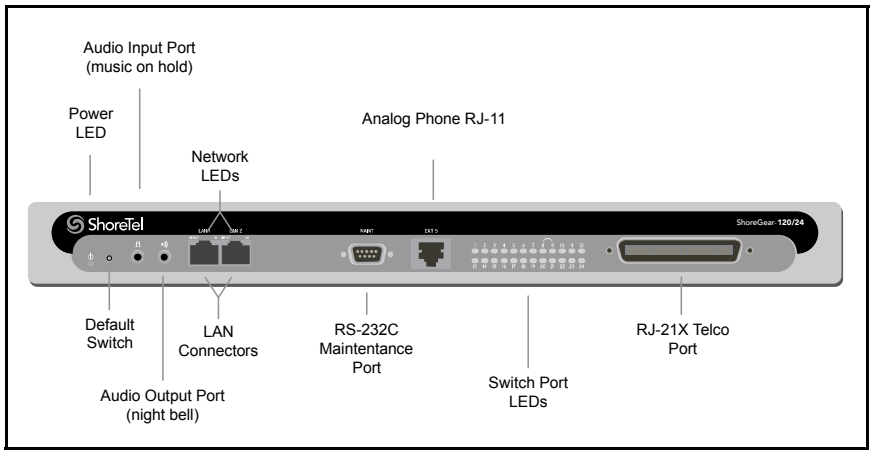

Figure C-15 ShoreGear 120 Front Plate

C.4.1.1 Switch Capacity

- **Analog Circuit Resources**
  - — *Ports 1-8:* Eight Loop Start Trunks, DID Trunks, or Extensions
  - — *Ports 9-24:* Sixteen Extensions.
  - — *Power Failure Transfer Unit:* Trunk Port 8 to Extension Port 9
- **Make Me Conference Resource:** 24 Ports
  - — *Ports 1-24*
- **Maximum IP Phone Resources:** 120 devices
  - — *Analog Port Reallocation:* 120

C.4.1.2 LED Descriptions

Power LED

The ShoreGear 120 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.

- — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
- — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
- — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsa/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsa/vxworks`.
- — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Switch Port LEDs

The ShoreGear 120 has 24 telephone/trunk port LEDs. The color of the LED indicates the port function:

- **Green** when the port is a telephone port.
- **Yellow** when the port is a trunk port.
- **Off** indicates the port is reserved for IP phones, for conferencing, or is unconfigured.

The following describes the switch port LED behavior and meaning:

- **Telephone Port LEDs (Green)**
  - — ***When on steady,*** the port is configured as a telephone port and the telephone is idle.
  - — ***When flashing with ring cadence,*** the telephone is ringing.
  - — ***When flashing slowly,*** the telephone is off hook.
  - — ***When flashing fast,*** the port is in use (call in progress).
- **Trunk Port LED (Yellow):**
  - — ***When on steady,*** the port is configured as a trunk port and the trunk is idle.
  - — ***When flashing slowly,*** the trunk is off hook.
  - — ***When flashing fast,*** the trunk is in use (call in progress).
- **Port LED Alternating Green/Yellow:** The port is out of service. The LED periodically alternates green/yellow or yellow/green. The color of the LED between alternating colors indicates the port type: green for phone and yellow for trunk.
- **Off (IP phone):** When the LED is off, the port is reserved for IP phones, for conferencing, or is unconfigured.

Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on*** (not flashing), heavy network activity is detected.
  - — ***When off***, the switch has no power.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green***, the switch is connected to a 100BaseT network.
  - — ***When off***, the switch is connected to a 10BaseT network.

C.4.1.3 ShoreGear 120 Connectors

The ShoreGear 120 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-11 connector for connecting an analog phone (extension 9)
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 8 to Extension Port 9
  - — ***Backup Operator:*** Extension Port 9

ShoreGear 120 RJ-21X Telephone and Trunk Connector

Table C-10 lists the RJ-21X Ring and Tip pin numbers for the SG 120I

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk, DID, Extension	1	Blue/White	26	White/Blue
2	Trunk, DID, Extension	2	Orange/White	27	White/Orange
3	Trunk, DID, Extension	3	Green/White	28	White/Green
4	Trunk, DID, Extension	4	Brown/White	29	White/Brown
5	Trunk, DID, Extension	5	Slate/White	30	White/Slate
6	Trunk, DID, Extension	6	Blue/Red	31	Red/Blue
7	Trunk, DID, Extension	7	Orange/Red	32	Red/Orange
8	Trunk, DID, Extension	8	Green/Red	33	Red/Green
9	Extension	9	Brown/Red	34	Red/Brown

Table C-10 ShoreGear 120 RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
10	Extension	10	Slate/Red	35	Red/Slate
11	Extension	11	Blue/Black	36	Black/Blue
12	Extension	12	Orange/Black	37	Black/Orange
13	Extension	13	Green/Black	38	Black/Green
14	Extension	14	Brown/Black	39	Black/Brown
15	Extension	15	Slate/Black	40	Black/Slate
16	Extension	16	Blue/Yellow	41	Yellow/Blue
17	Extension	17	Orange/Yellow	42	Yellow/Orange
18	Extension	18	Green/Yellow	43	Yellow/Green
19	Extension	19	Brown/Yellow	44	Yellow/Brown
20	Extension	20	Slate/Yellow	45	Yellow/Slate
21	Extension	21	Blue/Violet	46	Violet/Blue
22	Extension	22	Orange/Violet	47	Violet/Orange
23	Extension	23	Green/Violet	48	Violet/Green
24	Extension	24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-10 ShoreGear 120 RJ-21X Telephone and Trunk Connector Pins

C.4.2 ShoreGear 24A Voice Switch

The following sections describe ShoreGear 24A resource capacity, LED behavior, and connectors. The ShoreGear 24A is not supported in installations outside the U.S. and Canada. Figure C-16 displays the ShoreGear 24A front plate.

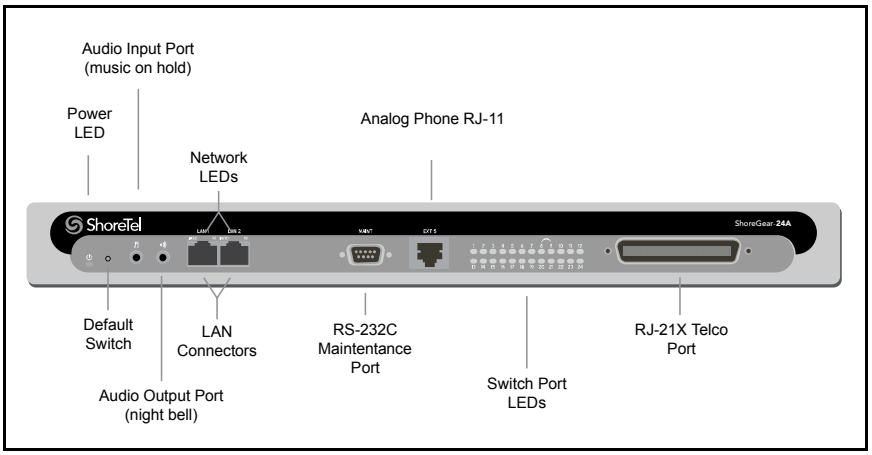

Figure C-16 ShoreGear 24A Front Plate

C.4.2.1 Switch Capacity

- Analog Circuit Resources
  - — *Ports 1-24:* Twenty four extensions
- Make Me Conference Resource: 24 Ports

— *Ports 1-24*

- **Maximum IP Phone Resources:** None

C.4.2.2 LED Descriptions

Power LED

The ShoreGear 24A has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsa/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsa/vxworks`.
  - — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Switch Port LEDs

The ShoreGear 24A has 24 telephone/trunk port LEDs. The color of the LED indicates the port function:

- **Green** when the port is a telephone port.
- **Yellow** when the port is a trunk port.
- **Off** indicates the port is reserved for IP phones, for conferencing, or is unconfigured.

The following describes the switch port LED behavior and meaning:

- **Telephone Port LEDs (Green)**
  - — *When on steady,* the port is configured as a telephone port and the telephone is idle.

  - — *When flashing with ring cadence,* the telephone is ringing.
  - — *When flashing slowly,* the telephone is off hook.
  - — *When flashing fast,* the port is in use (call in progress).
- **Trunk Port LED (Yellow):**
  - — *When on steady,* the port is configured as a trunk port and the trunk is idle.
  - — *When flashing slowly,* the trunk is off hook.
  - — *When flashing fast,* the trunk is in use (call in progress).
- **Port LED Alternating Green/Yellow:** The port is out of service. The LED periodically alternates green/yellow or yellow/green. The color of the LED between alternating colors indicates the port type: green for phone and yellow for trunk.
- **Off (IP phone):** When the LED is off, the port is reserved for IP phones, for conferencing, or is unconfigured.

Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — *When flashing,* network activity is detected.
  - — *When on* (not flashing), heavy network activity is detected.
  - — *When off*, the switch has no power.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — *When green*, the switch is connected to a 100BaseT network.
  - — *When off*, the switch is connected to a 10BaseT network.

C.4.2.3 ShoreGear 24A Connectors

The ShoreGear 24A voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-11 connector for connecting an analog phone (extension 9)
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports

ShoreGear 24A RJ-21X Telephone and Trunk Connector

Table C-11 lists the RJ-21X Ring and Tip pin numbers for the SG 24AI

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Extension	1	Blue/White	26	White/Blue
2	Extension	2	Orange/White	27	White/Orange
3	Extension	3	Green/White	28	White/Green
4	Extension	4	Brown/White	29	White/Brown
5	Extension	5	Slate/White	30	White/Slate
6	Extension	6	Blue/Red	31	Red/Blue
7	Extension	7	Orange/Red	32	Red/Orange
8	Extension	8	Green/Red	33	Red/Green
9	Extension	9	Brown/Red	34	Red/Brown
10	Extension	10	Slate/Red	35	Red/Slate
11	Extension	11	Blue/Black	36	Black/Blue
12	Extension	12	Orange/Black	37	Black/Orange
13	Extension	13	Green/Black	38	Black/Green
14	Extension	14	Brown/Black	39	Black/Brown
15	Extension	15	Slate/Black	40	Black/Slate
16	Extension	16	Blue/Yellow	41	Yellow/Blue
17	Extension	17	Orange/Yellow	42	Yellow/Orange
18	Extension	18	Green/Yellow	43	Yellow/Green
19	Extension	19	Brown/Yellow	44	Yellow/Brown
20	Extension	20	Slate/Yellow	45	Yellow/Slate
21	Extension	21	Blue/Violet	46	Violet/Blue
22	Extension	22	Orange/Violet	47	Violet/Orange
23	Extension	23	Green/Violet	48	Violet/Green
24	Extension	24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-11 ShoreGear 24A RJ-21X Telephone and Trunk Connector Pins

C.4.3 ShoreGear 60 Voice Switch

The following sections describe ShoreGear 60 resource capacity, LED behavior, and connectors. The ShoreGear 60 is not supported in installations outside the U.S. and Canada. Figure C-17 displays the ShoreGear 60 front plate.

The ShoreGear 60 is often referred to as the ShoreGear 60/12 (SG 60/12).

C.4.3.1 Switch Capacity

- **Analog Circuit Resources**
  - — ***Ports 1-8:*** Eight Loop Start Trunks, DID Trunks, or Extensions
  - — ***Ports 9-12:*** Four Extensions.
  - — ***Backup Operator:*** Extension Port 9
  - — ***Power Failure Transfer Unit:*** Trunk Port 8 to Extension Port 9
- **Make Me Conference Resource:** 12 ports

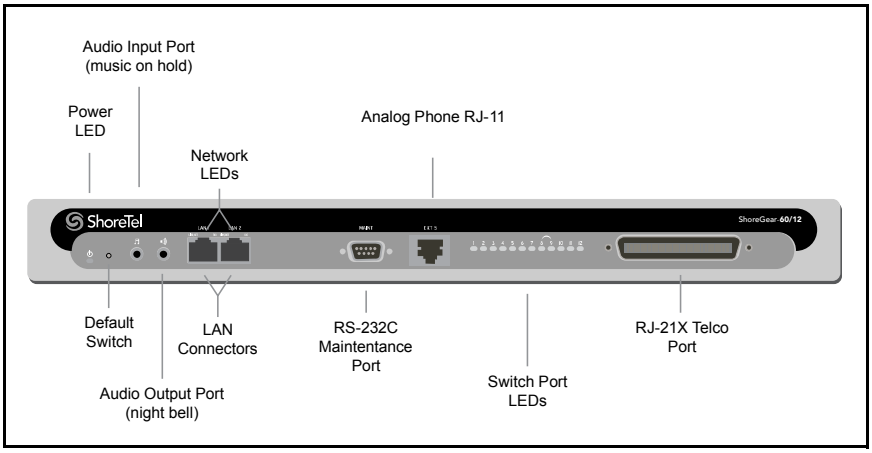

Figure C-17 ShoreGear 60 Front Plate

— *Ports 1-12*

- **Maximum IP Phone Resources:** 60 devices
  — *Analog Port Reallocation:* 60

C.4.3.2 LED Descriptions

Power LED

The ShoreGear 60 has one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  — *2 flashes*—The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  — *3 flashes*—Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to /tsa/vxworks. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to /tsa/vxworks.
  — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using

the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Switch Port LEDs

The ShoreGear 60 has 12 telephone/trunk port LEDs. The color of the LED indicates the port function:

- **Green** when the port is a telephone port.
- **Yellow** when the port is a trunk port.
- **Off** indicates the port is reserved for IP phones, for conferencing, or is unconfigured.

The following describes the switch port LED behavior and meaning:

- **Telephone Port LEDs (Green)**
  - ***When on steady,*** the port is configured as a telephone port and the telephone is idle.
  - ***When flashing with ring cadence,*** the telephone is ringing.
  - ***When flashing slowly,*** the telephone is off hook.
  - ***When flashing fast,*** the port is in use (call in progress).
- **Trunk Port LED (Yellow)**
  - ***When on steady,*** the port is configured as a trunk port and the trunk is idle.
  - ***When flashing slowly,*** the trunk is off hook.
  - ***When flashing fast,*** the trunk is in use (call in progress).
- **Port LED Alternating Green/Yellow:** The port is out of service. The LED periodically alternates green/yellow or yellow/green. The LED color between alternating colors indicates the port type: green for phone and yellow for trunk.
- **Off (IP phone):** When the LED is off, the port is reserved for IP phones, for conferencing, or is unconfigured.

Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - ***When flashing,*** network activity is detected.
  - ***When on*** (not flashing), heavy network activity is detected.
  - ***When off,*** the switch has no power.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - ***When green,*** the switch is connected to a 100BaseT network.
  - ***When off,*** the switch is connected to a 10BaseT network.

C.4.3.3 ShoreGear 60 Connectors

ShoreGear 60 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-11 connector for connecting an analog phone (extension 9)
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — *Power Failure Transfer Unit:* Trunk Port 8 to Extension Port 9
  - — *Backup Operator:* Extension Port 9

ShoreGear 60 RJ-21X Telephone and Trunk Connector

Table C-12 lists the RJ-21X Ring and Tip pin numbers for the SG 60.

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk, DID, Extension	1	Blue/White	26	White/Blue
2	Trunk, DID, Extension	2	Orange/White	27	White/Orange
3	Trunk, DID, Extension	3	Green/White	28	White/Green
4	Trunk, DID, Extension	4	Brown/White	29	White/Brown
5	Trunk, DID, Extension	5	Slate/White	30	White/Slate
6	Trunk, DID, Extension	6	Blue/Red	31	Red/Blue
7	Trunk, DID, Extension	7	Orange/Red	32	Red/Orange
8	Trunk, DID, Extension	8	Green/Red	33	Red/Green
9	Extension	9	Brown/Red	34	Red/Brown
10	Extension	10	Slate/Red	35	Red/Slate
11	Extension	11	Blue/Black	36	Black/Blue
12	Extension	12	Orange/Black	37	Black/Orange
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
–		21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
–		23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-12 ShoreGear 60 RJ-21X Telephone and Trunk Connector Pins

C.4.3.4 ShoreGear 40 Voice Switch

The following sections describe ShoreGear 40 resource capacity, LED behavior, and connectors. The ShoreGear 40 is not supported in installations outside the U.S. and Canada. Figure C-18 displays the ShoreGear 40 front plate.

The ShoreGear 40 is often referred to as the ShoreGear 40/8 (SG 40/8)

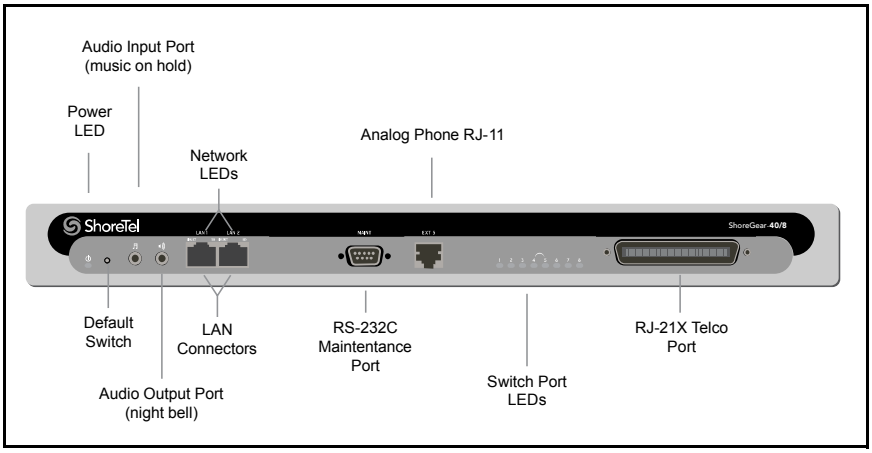

Figure C-18 ShoreGear 40 Front Plate

C.4.3.5 Switch Capacity

- **Analog Circuit Resources**
  - — ***Ports 1-2:*** Two Loop Start Trunks, DID Trunks, or Extensions
  - — ***Ports 3-4:*** Two Loop Start Trunks.
  - — ***Ports 5-8:*** Four Extensions
  - — ***Power Failure Transfer Unit:*** Trunk Port 4 to Extension Port 5
- **Make Me Conference Resource**: eight ports
  - — ***Ports 1-8***
- **Maximum IP Phone Resources**: 40 devices
  - — ***Analog Port Reallocation:*** 40

C.4.3.6 LED Descriptions

Power LED

The ShoreGear 40 has one power LED, which indicates the following:

- **On**: The switch is operating normally.
- **Off**: The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.

- — *4 flashes*—The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
- — *5 flashes*—The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/tsa/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/tsa/vxworks`.
- — *6 flashes*—Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Switch Port LEDs

The ShoreGear 40 has 8 telephone/trunk port LEDs. The color of the LED indicates the port function:

- **Green** when the port is a telephone port.
- **Yellow** when the port is a trunk port.
- **Off** indicates the port is reserved for IP phones, for conferencing, or is unconfigured.

The following describes the switch port LED behavior and meaning.

- **Telephone Port LEDs (Green)**
  - — *When on steady,* the port is configured as a telephone port and the telephone is idle.
  - — *When flashing with ring cadence,* the telephone is ringing.
  - — *When flashing slowly,* the telephone is off hook.
  - — *When flashing fast,* the port is in use (call in progress).
- **Trunk Port LED (Yellow)**
  - — *When on steady,* the port is configured as a trunk port and the trunk is idle.
  - — *When flashing slowly,* the trunk is off hook.
  - — *When flashing fast,* the trunk is in use (call in progress).
- **Port LED Alternating Green/Yellow:** The port is out of service. The LED periodically alternates green/yellow or yellow/green. The color of the LED between alternating colors indicates the port type: green for phone and yellow for trunk.
- **Off (IP phone):** When the LED is off, the port is reserved for IP phones, for conferencing, or is unconfigured.

Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity.

When both LAN connectors are connected into a redundant network configuration, one network port is active while the other is in standby mode. If one LAN connection fails, the switch activates the other port.

The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on*** (not flashing), heavy network activity is detected.
  - — ***When off,*** network activity is not detected.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.

C.4.3.7 ShoreGear 40 Connectors

The ShoreGear 40 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-11 connector for connecting an analog phone (extension 9)
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports
  - — ***Power Failure Transfer Unit:*** Trunk Port 4 to Extension Port 5
  - — ***Backup Operator:*** Extension Port 5

ShoreGear 40 RJ-21X Telephone and Trunk Connector

Table C-13 lists the RJ-21X Ring and Tip pin numbers for the SG 40I

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk, DID, Extension	1	Blue/White	26	White/Blue
2	Trunk, DID, Extension	2	Orange/White	27	White/Orange
3	Trunk	3	Green/White	28	White/Green
4	Trunk	4	Brown/White	29	White/Brown
5	Extension	5	Slate/White	30	White/Slate
6	Extension	6	Blue/Red	31	Red/Blue
7	Extension	7	Orange/Red	32	Red/Orange
8	Extension	8	Green/Red	33	Red/Green
–		9	Brown/Red	34	Red/Brown
–		10	Slate/Red	35	Red/Slate
–		11	Blue/Black	36	Black/Blue
–		12	Orange/Black	37	Black/Orange

Table C-13 ShoreGear 40 RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
–		13	Green/Black	38	Black/Green
–		14	Brown/Black	39	Black/Brown
–		15	Slate/Black	40	Black/Slate
–		16	Blue/Yellow	41	Yellow/Blue
–		17	Orange/Yellow	42	Yellow/Orange
–		18	Green/Yellow	43	Yellow/Green
–		19	Brown/Yellow	44	Yellow/Brown
–		20	Slate/Yellow	45	Yellow/Slate
–		21	Blue/Violet	46	Violet/Blue
–		22	Orange/Violet	47	Violet/Orange
–		23	Green/Violet	48	Violet/Green
–		24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-13 ShoreGear 40 RJ-21X Telephone and Trunk Connector Pins

C.4.4 ShoreGear-T1 and ShoreGear E1 Voice Switches

The following sections describe ShoreGear-T1 and ShoreGear E1 resource capacity, LED behavior, and connectors. The ShoreGear-T1 is not supported in installations outside the U.S. and Canada. Figure C-19 displays the ShoreGear-T1 front plate. The ShoreGear E1 front plate is identical to the ShoreGear-T1 except for the E1 labeling.

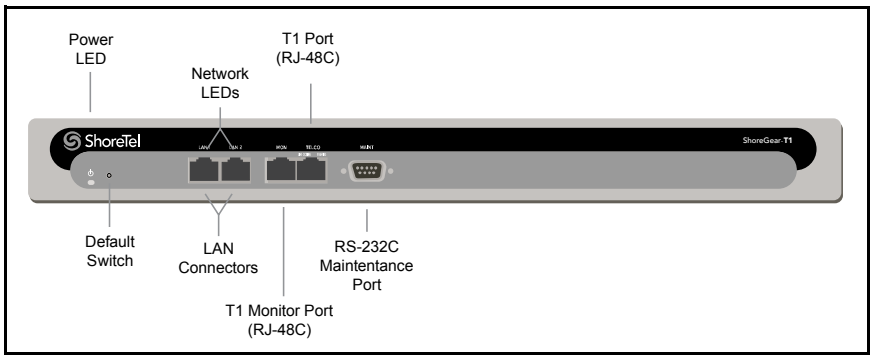

Figure C-19 ShoreGear-T1 Front Plate

The ShoreGear-T1 provides higher-density trunking to the central office using CAS or PRI signaling. The ShoreGear-T1 can also be used as a gateway to legacy PBX systems.

The ShoreGear E1 provides higher-density trunking to the central office using PRI signaling. The ShoreGear E1 can also be used as a gateway to legacy PBX systems.

C.4.4.1 Switch Capacity

- Digital Circuit Resources
  - — *SG T1 – One T1 circuit, 24 channels per circuit:* 24 channels maximum.
  - — *SG E1 – One T1 circuit, 30 channels per circuit:* 30 channels maximum.

- **Make Me Conference Resources:** None
- **Maximum IP Phone Resources:** None

C.4.4.2 LED Descriptions

Power LED

The ShoreGear-T1 and ShoreGear E1 voice switches have one power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes—***The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes—***Booting via FTP. Flash memory may be corrupted. Go to the **Quick Look** page to make sure that the system is running properly.
  - — ***4 flashes—***The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes—***The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds.
  - — ***6 flashes—***Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

The network LEDs (LAN1 and LAN2) indicate the speed at which the switch is communicating with the network and whether there is network activity. The network LED descriptions are as follows:

- **Link/Activity:** When lit, this LED indicates that the switch is connected to an Ethernet network. This LED indicates network activity, as follows:
  - — ***When flashing,*** network activity is detected.
  - — ***When on*** (not flashing), heavy network activity is detected.
  - — ***When off,*** network activity is not detected.

  This LED is not directly related to any switch's individual network activity. For example, if three switches are connected to the same hub and one switch's Traffic LED shows activity, the other switches will indicate the same activity.
- **100M**
  - — ***When green,*** the switch is connected to a 100BaseT network.

— ***When off,*** the switch is connected to a 10BaseT network.

Monitor and Telco LEDs

The Monitor and Telco LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. The Monitor and Telco LED descriptions follow.

Telco and Monitor LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are being received at one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the Central Office.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits.
  - — ***When flashing slow yellow,*** a small number of frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** a series of frame-bit errors (>1 per 1000) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When flashing red,*** loopback is active (local or CO).
  - — ***When off,*** the switch has no power.

ShoreGear-T1 and ShoreGear E1 Connectors

The ShoreGear-T1 and ShoreGear E1 voice switches contain the following components:

- 1 DB-9 female connector for maintenance
- 2 RJ-45 connectors for the LAN interface
- 1 RJ-45 T1 telco port
- 1 RJ-45 T1 monitor port for connecting test equipment

C.5 Specification – IPBX Switches

C.5.1 IPBX-24 Voice Switch

The IPBX-24 (Figure C-20) supports 24 analog ports in a combination of no more then 8 standard trunk ports and 16 analog telephone ports, up to 24. The IPBX-24 interfaces to standard analog trunks using loop start or wink start signaling, as well as to standard analog telephones, including CLASS feature phones with Caller ID Name and Number, and Message Waiting.

The IPBX-24 can be configured to support up to 120 ShoreTel IP phones (five IP phones per IP phone port). The IPBX-24 ports are configured for IP through the ***Edit ShoreGear 24*** page.

If you are installing IP phones in your system, you must assign sufficient IPBX-24 ports to IP phone support before attempting to install and configure IP phones.

The IPBX-24 does not support analog trunks outside the U.S. and Canada. The IPBX-24 does not support Caller ID, Message Waiting, Fax, and modems outside the U.S. and Canada.

The IPBX-24 LEDs and connectors are defined below.

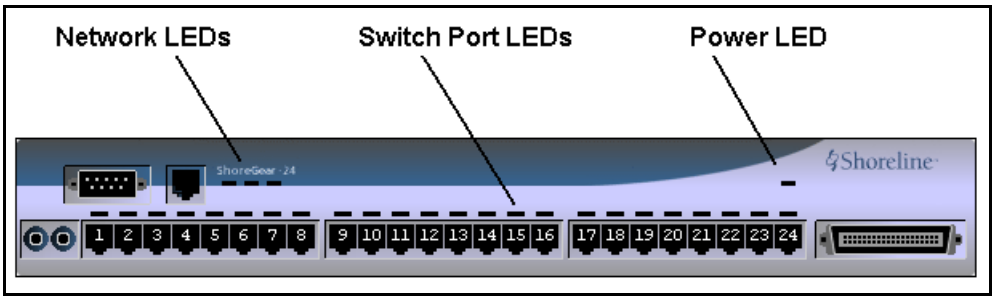

Figure C-20 IPBX-24 Front Plate

C.5.1.1 LED Descriptions

Power LED

The IPBX-24 has one green power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory might be corrupted. Go to the **Quick Look** page to ensure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.

— ***5 flashes—***The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds. You can use BOOTP or DHCP to tell the switch where the files are. If you are using BOOTP, set the BOOTP server to the IP address of the ShoreWare server, and set the boot file to `/ts24/vxworks`. If you are using a DHCP server that supports options 66 and 67, set option 66 to the ShoreWare server's IP address, and set option 67 to `/ts24/vxworks`.

— ***6 flashes—***Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Switch Port LEDs

The IPBX-24 has 24 telephone/trunk port LEDs. The color of the LED indicates the port function:

- **Green** when the port is a telephone port.
- **Yellow** when the port is a trunk port.
- **Off** indicates the port is reserved for IP phones, for conferencing, or is unconfigured.

The following describes the switch port LED behavior and meaning:

- **Telephone Port LEDs (Green)**
  - — ***When on steady,*** the port is configured as a telephone port and the telephone is idle.
  - — ***When flashing with ring cadence,*** the telephone is ringing.
  - — ***When flashing slowly,*** the telephone is off hook.
  - — ***When flashing fast,*** the port is in use (call in progress).
- **Trunk Port LED (Yellow)**
  - — ***When on steady,*** the port is configured as a trunk port and the trunk is idle.
  - — ***When flashing slowly,*** the trunk is off hook.
  - — ***When flashing fast,*** the trunk is in use (call in progress).
- **Port LED (Red):** When on, the port is out of service.
- **IP Phone (Off):** When the LED is off, the port is reserved for IP phones, for conferencing, or is unconfigured.

Network LEDs

The network LEDs indicate the speed at which the switch is communicating with the network and whether there is network activity.

The network LED descriptions are as follows:

- **Link:** When lit, the switch is connected to an Ethernet network.
- **100M**
  - — ***When lit,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.
- **Traffic:** This LED indicates network activity, as follows:

— ***When flashing,*** network activity is detected.
— ***When on (not flashing),*** heavy network activity is detected.
— ***When off,*** network activity is not detected.

This LED is not directly related to any particular switch's individual network activity. For example, if you have three switches that are connected to the same hub, and one switch's Traffic LED shows activity, the other switches will indicate the same.

C.5.1.2 IPBX-24 Connectors

The IPBX-24 voice switch contains the following components:

- 1 3.5 mm mono connector for audio input (music on hold)
- 1 3.5 mm mono connector for audio output (overhead paging and night bell)
- 1 DB-9 female connector for maintenance
- 1 RJ-45 connector for the LAN interface
- 24 RJ-11 connectors for the trunk and telephone ports:
  — 8 universal telephone/trunk ports (Ports 1 through 8)
  — 16 telephone ports (Ports 9 through 24)
  — Power fail transfer (between Ports 8 and 9)
- 1 RJ-21X male connector for mass termination of the telephone/trunk ports

IPBX-24 RJ-21X Telephone and Trunk Connector

Table C-14 lists the RJ-21X Ring and Tip pin numbers for the IPBX-24I

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
1	Trunk, DID, Extension	1	Blue/White	26	White/Blue
2	Trunk, DID, Extension	2	Orange/White	27	White/Orange
3	Trunk, DID, Extension	3	Green/White	28	White/Green
4	Trunk, DID, Extension	4	Brown/White	29	White/Brown
5	Trunk, DID, Extension	5	Slate/White	30	White/Slate
6	Trunk, DID, Extension	6	Blue/Red	31	Red/Blue
7	Trunk, DID, Extension	7	Orange/Red	32	Red/Orange
8	Trunk, DID, Extension	8	Green/Red	33	Red/Green
9	Extension	9	Brown/Red	34	Red/Brown
10	Extension	10	Slate/Red	35	Red/Slate
11	Extension	11	Blue/Black	36	Black/Blue
12	Extension	12	Orange/Black	37	Black/Orange
13	Extension	13	Green/Black	38	Black/Green
14	Extension	14	Brown/Black	39	Black/Brown
15	Extension	15	Slate/Black	40	Black/Slate
16	Extension	16	Blue/Yellow	41	Yellow/Blue
17	Extension	17	Orange/Yellow	42	Yellow/Orange
18	Extension	18	Green/Yellow	43	Yellow/Green
19	Extension	19	Brown/Yellow	44	Yellow/Brown
20	Extension	20	Slate/Yellow	45	Yellow/Slate

Table C-14 IPBX-24 RJ-21X Telephone and Trunk Connector Pins

Port	Type	Ring		Tip	
		Pin #	Cable Color	Pin #	Cable Color
21	Extension	21	Blue/Violet	46	Violet/Blue
22	Extension	22	Orange/Violet	47	Violet/Orange
23	Extension	23	Green/Violet	48	Violet/Green
24	Extension	24	Brown/Violet	49	Violet/Brown
–		25	Slate/Violet	50	Violet/Slate

Table C-14 IPBX-24 RJ-21X Telephone and Trunk Connector Pins

C.5.2 IPBX-T1 and IPBX-E1 Voice Switch

The IPBX-T1 (Figure C-15) provides higher-density trunking to the central office using T1 or PRI signaling. The IPBX-E1 provides higher-density trunking using E1 PRI signaling.

The IPBX-T1 and IPBX-E1 LEDs and connectors are defined below.

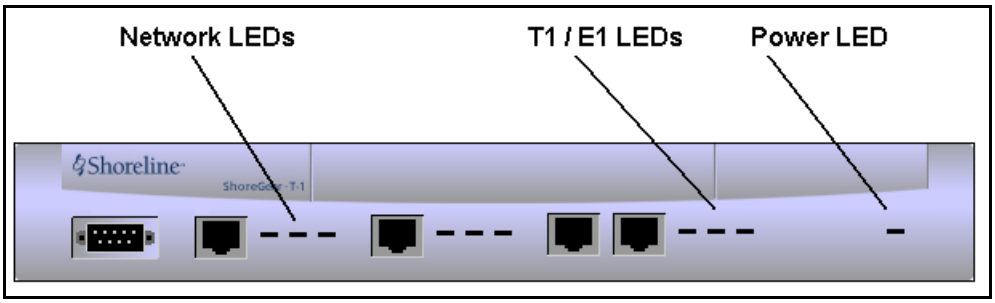

Table C-15 ShoreGear T1 and ShoreGear E1 Front Panel

C.5.2.1 LED Descriptions

Power LED

The IPBX-T1 and IPBX-E1 have one red power LED, which indicates the following:

- **On:** The switch is operating normally.
- **Off:** The switch has no power.
- **Flashing**
  - — ***2 flashes*—**The switch failed its internal self-test. This indicates a hardware failure; replace the unit and submit a Return Material Authorization (RMA) to ShoreTel, Inc.
  - — ***3 flashes*—**Booting via FTP. Flash memory may be corrupted. Go to the **Quick Look** page to make sure that the system is running properly.
  - — ***4 flashes*—**The IP address is unavailable. DHCP and BOOTP did not respond to the IP address request, and the IP address is not available in nonvolatile memory to continue boot process. The switch will automatically reboot in five seconds and try again. Check the BOOTP/DHCP server and the network configuration to ensure that the voice switch is receiving a valid IP address.
  - — ***5 flashes*—**The operating system is not available. The switch is booting from FTP but cannot find the boot files. It automatically reboots in five seconds.

— ***6 flashes—***Using a previously stored IP address. A BOOTP/DHCP transaction was attempted, but the BOOTP/DHCP server did not respond. The switch continues to use the IP address stored in nonvolatile memory until it receives a valid response. If the switch receives a response that provides a different IP address, it reboots using the new IP address. If the switch receives a response that matches the IP address stored in nonvolatile memory, it continues operation, and the power LED stops flashing. If the problem persists, check the BOOTP/DHCP server and network configuration.

Network LEDs

Network LEDs indicate the speed at which the switch is communicating with the network and when there is network activity. The network LED descriptions follow:

- **Link:** This LED indicates that the switch is connected to an Ethernet network.
- **100M**
  - — ***When lit,*** the switch is connected to a 100BaseT network.
  - — ***When off,*** the switch is connected to a 10BaseT network.
- **Traffic:** This LED indicates network activity, as follows:
  - — When flashing, network activity is detected.
  - — When on (not flashing), heavy network activity is detected.
  - — When off, network activity is not detected.

  This LED is not directly related to any particular switch's individual network activity. For example, if you have three switches connected to the same hub, and one switch's Traffic LED shows activity, the other switches will indicate the same.

T1 and E1 LEDs

The T1 and E1 LEDs indicate line coding, network framing, and loopback status. These LEDs are color coded—green, yellow, and red. T1 and E1 LED alarms and errors are logged as switch events in ShoreWare Director's event log.

- **Line Coding:** This LED indicates line coding status, as follows:
  - — ***When green,*** the line coding signal is good.
  - — ***When yellow,*** bipolar violations (BPV) are detected one second intervals.
  - — ***When red,*** a loss of signal (LOS) has occurred.
  - — ***When off,*** the switch has no power.
- **Framing:** This LED indicates network framing status, as follows:
  - — ***When green,*** the T1/E1 signal is *in frame*; the signal is synchronized.
  - — ***When yellow,*** a *yellow alarm* has been received from the CO.
  - — ***When flashing yellow,*** the frame-bit error rate has exceeded its limits.
  - — ***When flashing slow yellow,*** frame-bit errors (>1 per million) have occurred; this state will take up to 10 minutes to clear.
  - — ***When flashing fast yellow,*** frame-bit errors (>1 per 1000) have occurred.
  - — ***When red,*** the T1/E1 signal is out-of-frame (OOF). The received signal cannot be framed to the Extended Superframe (ESF) or D4 format.
  - — ***When off,*** the switch has no power.
- **Loopback:** This LED indicates loopback status for testing, as follows:
  - — ***When yellow,*** loopback is enabled. This may be set from within ShoreWare Director or from the CO.
  - — ***When off,*** loopback is disabled.

C.5.2.2 IPBX-T1 and IPBX-E1 Connectors

The IPBX-T1 and IPBX-E1 voice switches contain the following components:

- 1 DB-9 female connector for maintenance
- 1 RJ-45 connector for the LAN interface
- 1 RJ-48C connector for T1 or E1 monitoring
- 1 RJ-48C connector for the T1 or E1 interface